

**Collège d'experts chargé du contrôle
des systèmes de vote et de dépouillement
automatisés**

Rapport concernant les élections du 18 mai 2003

2 juin 2003

Table des matières

1	Composition du collège.....	3
2	La mission	4
2.1	La loi	4
2.2	Application de la loi	5
3	Aperçu des différents systèmes	6
3.1	Le vote automatisé	6
3.1.1	La nouvelle loi électorale	6
3.1.2	Modifications techniques générales	6
3.1.2.1	Ajout d'écrans d'information complémentaires.....	6
3.1.2.2	Utilisation de l'algorithme Rijndael.....	7
3.1.3	Expérience de ticketing dans les cantons de Waarschoot et Verlaine.....	7
3.2	Le dépouillement automatisé des votes par lecture optique: le système Favor de Fabricom.....	8
3.2.1	Le bureau principal de canton	8
3.2.1.1	La procédure.....	8
3.2.1.2	Le système de totalisation de Favor : matériel.....	8
3.2.1.3	Le système de totalisation Favor : fonctionnement.....	9
3.2.2	Préparation avec Favor.....	10
4	Méthode de contrôle.....	11
4.1	Les logiciels de vote sont conformes aux codes sources.....	11
4.2	La machine à voter ne retient pas le vote émis, la carte magnétique bien	11
4.3	Contrôle du système de dépouillement optique	11
5	Constatations	12
5.1	Intervention du Bureau Van Dijk.....	12
5.2	Les améliorations au système de lecture optique (Favor).....	12
5.3	Constatations à l'occasion des élections du 18 mai 2003	13
5.3.1	Fabrications des disquettes.....	13
5.3.2	Démonstrations et tests effectués avant les élections.....	13
5.3.3	La compilation de référence du 7 mai 2003	13
5.3.4	Analyse code de source	14
5.3.4.1	Digivote.....	15
5.3.4.2	Jites.....	15
5.3.4.3	Favor.....	16
5.3.5	Constatations le jour des élections	16
5.3.5.1	Contrôle dans les bureaux de vote.....	16
5.3.5.2	Remarques particulières	17
5.3.5.3	Remarques générales.....	18
5.3.6	Contrôles effectués après les élections.....	18
5.3.7	L'incident de Schaerbeek.....	19
5.3.7.1	Analyse technique du problème	19
5.3.7.2	Analyse détaillée du code source suite à l'incident de Schaerbeek.....	20
5.3.7.3	Conclusions du collège sur l'incident de Schaerbeek.....	20
6	Conclusions	21

1 Composition du collège

En application de l'article 5bis, § 1er, de la loi du 11 avril 1994 organisant le vote automatisé, ont été désignés pour contrôler l'utilisation et le bon fonctionnement des systèmes de vote et de totalisation automatisés lors des prochaines élections des Chambres législatives fédérales, les experts dont les noms suivent :

1. Experts désignés par la Chambre des représentants :
 - effectifs: MM. Freddy TOMICKI et Maurice ROBERT;
2. Experts désignés par le Sénat :
 - effectifs: MM. Emmanuel WILLEMS et Wim VERHAEST;
3. Expert désigné par le Conseil régional wallon :
 - effectif: M. Jean-Pierre GILSON;
4. Experts désignés par le Conseil flamand :
 - effectif: M. Robby DEBOELPAEP
 - suppléant: M. Bart MARTENS;
5. Experts désignés par le Conseil de la Communauté germanophone :
 - effectif: M. Bruno HICK
 - suppléant: M. Daniel BRANDT .

Ces experts forment le collège d'experts.

En application de l'alinéa 3 du même article 5bis, §1er, ont été désignés comme président M. Emmanuel WILLEMS et comme secrétaire M. Freddy TOMICKI.

2 La mission

2.1 La loi

Cette mission est réglée par l'article 5bis de la loi du 11 avril 1994. Les modifications principales dans la loi par rapport à la mission de contrôle antérieure (élections 2000) concernant la mission sont imprimées dans le texte suivant en gras :

<< Art. 5bis. §1er. Lors de l'élection des membres de la Chambre des représentants et du Sénat, du Parlement européen et des conseils de région et de communauté ainsi que des conseils provinciaux et communaux, des conseils de district et de l'aide sociale.

1° la Chambre des représentants, le Sénat et le Conseil de la Région de Bruxelles-Capitale peuvent désigner chacun deux experts effectifs et deux experts suppléants;

2° le Conseil régional wallon, le Conseil flamand et le Conseil de la Communauté germanophone peuvent désigner chacun un expert effectif et un expert suppléant.

Ces désignations peuvent être effectuées tant lors du renouvellement complet de chaque assemblée que lors d'une nouvelle élection organisée suite à l'annulation d'un scrutin, ainsi que lors d'une élection suite à une vacance à laquelle il ne peut être pourvu par l'installation d'un suppléant.

Les personnes visées au premier alinéa forment le collège d'experts. **Ils désignent en leur sein un président et un secrétaire.**

§2. Ces experts contrôlent lors des élections l'utilisation et le bon fonctionnement de l'ensemble de systèmes de vote et de dépouillement automatisés ainsi que les procédures concernant la confection, la distribution et l'utilisation des appareils, des logiciels et des supports d'information électroniques. Les experts reçoivent du ministère de l'Intérieur le matériel ainsi que l'ensemble des données, renseignements et informations utiles pour exercer un contrôle sur les systèmes de vote et de dépouillement automatisés. Ils peuvent notamment vérifier la fiabilité des logiciels des machines à voter, la transcription exacte des votes émis sur la carte magnétique, **la transcription exacte pour l'urne électronique des suffrages exprimés sur le support de mémoire du bureau de vote, l'enregistrement exact du support de mémoire provenant du bureau de vote sur le support de mémoire destiné à la totalisation des votes, la totalisation des suffrages exprimés**, la lecture optique des votes exprimés et **le système de contrôle du vote automatisé par impression des suffrages émis sur support papier.**

Ils effectuent ce contrôle à partir du 40e jour précédant l'élection, le jour de l'élection et après celle-ci, jusqu'au dépôt du rapport visé au § 3.

§3. 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 et le Sénat, les conseils régionaux et communautaires et le Parlement européen, les experts remettent un rapport au ministre de l'Intérieur ainsi qu'aux assemblées législatives fédérales, régionales et communautaires. Au plus tard dix jours après la clôture des scrutins et en tout état de cause avant la validation des élections pour ce qui concerne les conseils provinciaux, communaux, de district et de l'aide sociale, ils remettent un rapport au ministre de l'Intérieur et aux assemblées législatives fédérales.

Leur rapport peut notamment comprendre des recommandations relatives au matériel et aux logiciels utilisés.

§4. Les experts sont tenus au secret. Toute violation de ce secret sera sanctionnée conformément à l'article 458 du Code pénal. >>

2.2 Application de la loi

Le collège regrette que, comme à l'occasion des élections du 8 octobre 2000, certaines assemblées n'aient pas désigné d'experts effectifs et/ou suppléants. L'exécution de la mission de contrôle s'en est ressentie.

Le collège regrette que certaines assemblées n'accordent pas plus d'importance à cette mission de contrôle.

Bien que le collège d'experts ait soulevé ce point à l'occasion du contrôle effectué lors des précédentes élections, le rôle des membres suppléants prévus par l'article 5bis §1er, n'est toujours pas clairement défini. La dernière phrase de ce paragraphe dispose que les membres effectifs et les membres suppléants forment ensemble le collège. Quelle est alors la différence entre ceux-ci? Le collège a, à nouveau, opté pour l'interprétation la plus large et considère les membres suppléants comme membres de plein droit du collège, avec les mêmes pouvoirs de contrôle.

Une fois de plus, le collège constate que sa mission engendre à la fois de réelles responsabilités et un surplus non négligeable de travail. L'incident de Schaerbeek a demandé plusieurs jours de travail afin d'en déterminer l'origine et la portée, ainsi que l'évaluation du risque que pareil incident se soit produit ailleurs sans être détecté. Considérant que tous les experts sont également fonctionnaires de leurs assemblées parlementaires respectives, il est essentiel que celles-ci (et en particulier leurs administrations) prennent conscience de l'importance de leur mission et qu'elles mettent à leur disposition le temps et les moyens nécessaires à son accomplissement.

3 Aperçu des différents systèmes

3.1 Le vote automatisé

Un système de vote automatisé se compose de différents éléments dont la machine à voter dans l'isoloir, qui est la partie la plus visible pour l'électeur, ne constitue qu'un élément. En effet, il y a plusieurs phases dans le processus électoral et à chaque phase correspond un sous-système bien déterminé du système de vote automatisé. Il y a d'abord la préparation pendant les semaines qui précèdent les élections, au cours de laquelle le constructeur du système de vote automatisé et le SPF Intérieur jouent un rôle. Le jour des élections, il y a la procédure dans les bureaux de vote. Le soir des élections enfin, on assiste à une troisième phase du vote automatisé dans les bureaux principaux où les votes sont totalisés. Il n'y a plus de bureaux de dépouillement.

Pour une description complète des systèmes utilisés (d'une part le système Digivote de la firme Steria et d'autre part le système Jites de la firme Stesud), nous renvoyons aux rapports du collège des experts relatifs aux élections de 1999 et 2000.

Le présent rapport ne s'attache qu'aux différences par rapport aux élections précédentes.

3.1.1 La nouvelle loi électorale

Les modifications de la loi électorale n'ont en soi pas d'influence sur l'utilisation des systèmes. La réintroduction des suppléants implique un retour au système tel qu'il existait avant les élections de 1999. Toutes les autres modifications ont seulement une influence sur la répartition des voix exprimées, matière qui sort du cadre de la mission du collège.

3.1.2 Modifications techniques générales

Les modifications principales concernent l'ajout de quelques écrans d'information ainsi que l'utilisation de l'algorithme Rijndael. Ces modifications ont été apportées aux deux systèmes.

3.1.2.1 Ajout d'écrans d'information complémentaires

L'ajout d'écrans d'information est une opération technique limitée qui en soi n'a que peu d'influence sur le fonctionnement du logiciel et du matériel. La conséquence principale est l'augmentation significative du temps moyen nécessaire au vote.

L'un des écrans d'informations supplémentaires indique à l'électeur que celui-ci peut visualiser à nouveau le vote qu'il a effectué. L'une des recommandations figurant dans les rapports précédents du collège a été ainsi suivie d'effet.

L'on ne peut faire abstraction du fait que l'augmentation du temps nécessaire pour effectuer un vote a une influence importante sur le fonctionnement des bureaux de vote.

Une confrontation des avantages (convivialité accrue) et des inconvénients (durée de vote allongée) est certainement conseillée à l'avenir.

3.1.2.2 Utilisation de l'algorithme Rijndael

L'algorithme d'encryption Rijndael AES (Advanced Encryption Standard) a été inclus par les deux fournisseurs dans les systèmes.

Le développement de l'algorithme Rijndael (par Joan Daemen et Vincent Rijmen Katholieke Universiteit Leuven) fait suite à l'appel public lancé pour la mise en place du nouvel AES par le US National Institute for Security (NIST).

L'algorithme est considéré comme l'un des mécanismes les plus sûrs qui soient naturellement disponibles.

L'un des avantages importants des mécanismes est que le code source des programmes a été publié entièrement et avant les élections sur Internet.

3.1.3 Expérience de ticketing dans les cantons de Waarschoot et Verlaine

Dans la perspective d'une augmentation de la transparence pour l'électeur, une expérience a été menée dans les cantons de Waarschoot (système Digivote) et Verlaine (système Jites). Le système de ticketing n'est qu'une extension des systèmes existants. Après que l'électeur ait exprimé son vote, un ticket est imprimé sur un système d'impression spécifique, ticket reprenant les voix pour la Chambre et pour le Sénat. Dans le même temps, le système montre à nouveau le vote exprimé à l'écran (il s'agit du même procédé que dans les autres bureaux de vote pour la visualisation des votes). L'électeur contrôle alors le vote repris sur le ticket au travers d'une vitre loupe. S'il confirme la concordance, l'électeur confirme son vote et la mention 'ACCORD' est alors imprimée sur le ticket, ce dernier est ensuite sectionné et tombe dans une urne scellée.

Si l'électeur marque son désaccord, l'alarme de la machine à voter se déclenche et le président du bureau doit intervenir. Si le président constate la concordance entre le vote émis et l'impression de celui-ci, il confirme le vote et la mention 'ACCORD' est alors imprimée sur le ticket, ce dernier est ensuite sectionné et tombe dans une urne scellée. Le ticket ne sort à aucun moment de l'équipement imprimante-urne.

L'électeur n'a donc à aucun moment accès à ce ticket et ne peut donc pas le modifier. La totalisation des bureaux de vote s'effectue dans un premier temps de façon semblable à celle des autres bureaux de totalisation. Ensuite, tous les tickets des différentes urnes sont mélangés et comptés manuellement à titre de contrôle du vote électronique.

Le vote est également imprimé sur le ticket sous forme de code à barres. Ceci permet un recomptage en cas de divergence entre les résultats du comptage manuel et du comptage automatisé. Cette possibilité a été ajoutée pour des raisons pratiques mais n'est pas prévue dans la réglementation légale.

3.2 Le dépouillement automatisé des votes par lecture optique: le système Favor de Fabricom

3.2.1 Le bureau principal de canton

3.2.1.1 La procédure

Dans les bureaux de vote, les votes se déroulent de manière traditionnelle; deux différences doivent cependant être mises en évidence concernant les bulletins de vote:

- Les deux coins supérieurs sont coupés d'une façon symétrique.
- En bas du bulletin de vote se trouvent des traits de référence verticaux en dessous des cases de vote.

Après la clôture du bureau de vote, les urnes sont transportées au bureau principal de canton ou de commune où les bulletins de vote seront dépouillés.

Le nombre de bulletins de vote par urne est d'abord compté.

Ensuite, les membres du bureau déplient les bulletins avec les votes émis vers l'extérieur. En même temps il est vérifié que les formes et dimensions des bulletins n'ont pas été altérées, qu'ils ne contiennent pas à l'intérieur un papier ou un objet quelconque, ou encore que l'auteur ne l'a pas rendu reconnaissable par un signe, une rature ou une marque non autorisés par la loi. Les bulletins altérés sont déclarés nuls et mis à part. Le total des votes nuls est encodé manuellement dans le système.

Les bulletins restants sont mis en plusieurs tas selon la capacité de la machine pour être dépouillés.

Tous les bulletins non blancs dépouillés correctement arrivent dans le premier bac de sortie. Les autres bulletins sont déviés vers le second bac de sortie. Pour ces derniers, il faut séparer les bulletins blancs qui ont aussi été dépouillés correctement des autres qui doivent être contrôlés et dépouillés manuellement. Procéder ainsi est plus facile car la quantité de bulletins dans le second bac est nettement plus faible que dans le premier bac.

Si un électeur vote en même temps en tête de liste et pour un ou plusieurs candidats de la même liste, il n'est pas tenu compte du vote en tête de liste.

Cette exception est autorisée par la loi.

3.2.1.2 Le système de totalisation de Favor : matériel

Un système automatisé de dépouillement des votes par lecture optique est installé par canton et par commune.

Chaque système de dépouillement est composé :

- d'un PC tournant sous Windows 9x, muni d'un écran 15", d'un clavier et d'une souris;
- d'un logiciel de dépouillement;
- d'une imprimante;

- d'un lecteur optique OMR (Optical Mark Reader);
- d'une alimentation de secours (UPS).

Chaque PC est identifié d'une façon unique et toutes les disquettes générées par un PC sont identifiées de la même façon; le logiciel de dépouillement est protégé par un mot de passe.

Le lecteur optique

La technique utilisée par le lecteur optique n'est pas celle de la reconnaissance des caractères mais celle de marques. En outre, des traits de référence verticaux situés en dessous des cases de vote sur les bulletins indiquent les endroits où le lecteur optique doit lire.

La lecture optique se fait recto-verso, les bulletins de vote étant pliés en deux afin que les votes exprimés soient visibles.

Le traitement des bulletins se fait à une cadence de plus de 50 bulletins par minute. Sans trop de perte de temps, on peut dépouiller 3 000 bulletins par heure.

Si l'électeur émet un vote valable, le lecteur le considère comme tel car les marques sont faites dans les cases prévues. Si l'électeur écrit un commentaire sur son bulletin de vote, celui-ci sera considéré comme nul. Si le commentaire est écrit dans les zones verticales entre les traits de référence où il n'y a pas de détection, la machine considère le vote comme valable. Étant donné que les membres du bureau de dépouillement trient les bulletins au préalable, les bulletins non-valides doivent être découverts au préalable.

Si un bulletin mal plié est introduit, le PC le signale de manière audible et demande de le ré-introduire correctement. De plus, une liste conviviale des incidents et remèdes à y apporter est fournie.

Lors d'un incident (lors de la lecture optique ou lors de l'écriture) comme une panne de courant, toute l'urne sera recomptée.

3.2.1.3 Le système de totalisation Favor : fonctionnement

Le système crée un tableau comportant les suffrages exprimés par liste pour chaque candidat. Ce tableau est inaccessible pendant la durée de l'enregistrement. Le tableau avec les suffrages exprimés doit pouvoir contenir l'expression du vote d'au moins 800 électeurs. Il permet d'enregistrer le choix jusqu'à 20 listes et 39 candidats par liste.

Pendant le traitement d'une urne, les données sont conservées dans la mémoire vive. Lorsque tous les paquets de l'urne sont traités, le système demande une confirmation pour enregistrer toutes les données sur le disque dur et sur la disquette de secours. A ce moment, il faut également mentionner combien de bulletins n'ont pas été comptés par la machine mais ont été considérés préalablement comme nuls par les membres du bureau (bulletins déchirés ou décrits comme illégaux).

Ce n'est que lorsque tous les bureaux sont totalisés que le traitement peut être clos. Plusieurs procès-verbaux sont imprimés et des disquettes sont créées.

Les principaux facteurs qui déterminent les limites de l'utilisation de ce système sont le nombre de listes et de candidats, la lisibilité des bulletins et la vitesse de lecture d'un bulletin.

3.2.2 Préparation avec Favor

Lors de l'initialisation, les données suivantes sont introduites :

- la date de l'élection;
- le type d'élection;
- le nombre d'urnes à traiter ainsi que les numéros des bureaux de vote correspondants;
- le nombre de listes électorales ainsi que, par liste électorale, le sigle, le numéro de la liste, le nombre de candidats et les coordonnées de la case de tête;
- liste électorale et par candidat, le nom, le numéro d'ordre sur la liste et les coordonnées de la case de vote sur le bulletin.

Lors de l'installation il faut également calibrer la sensibilité du lecteur optique. En outre le PC chargera les paramètres de calibrage dans le lecteur après chaque opération de lecture. Pendant tout le traitement c'est le PC qui gère le lecteur en non l'inverse. Ainsi, c'est le programme qui provoque le rejet du bulletin lors de l'absence de détection par une tête de lecture.

4 Méthode de contrôle

La méthode de contrôle ne diffère pas essentiellement de celle mise en oeuvre lors des élections précédentes.

Voici résumés les différents aspects contrôlés.

4.1 Les logiciels de vote sont conformes aux codes sources.

Le SPF Intérieur a divulgué le code source des systèmes via l'Internet. Ainsi, le citoyen se voit offrir la possibilité de contrôler les programmes. Le collègue a assisté à la compilation de référence au cours de laquelle furent générés les exécutables identiques à ceux distribués dans les différents bureaux de vote. Le code source utilisé est identique à celui publié sur l'Internet.

Au moyen de contrôles ponctuels dans les bureaux de vote visités, les experts ont pris des copies des disquettes "master" et "backup". Les logiciels utilisés furent ultérieurement comparés avec les copies à la disposition du collègue. Il fut ainsi possible de s'assurer que les logiciels utilisés étaient bien ceux portés à la connaissance du citoyen.

4.2 La machine à voter ne retient pas le vote émis, la carte magnétique bien.

Afin de contrôler cet aspect, un vote de référence a été émis en présence de témoins dans les bureaux de votes visités. Le vote émis a été visualisé sur une autre machine à voter.

Quelques jours après l'élection, les votes de référence émis furent à nouveau visualisés sur une installation de test, à partir des cartes magnétiques emportées.

4.3 Contrôle du système de dépouillement optique

Comme pour les systèmes de vote automatisés, il a été procédé à une épreuve de recompilation du logiciel à partir du code source déposé au coffre du SPF Intérieur, afin de comparer l'exécutable obtenu avec celui utilisé le jour des élections.

5 Constatations

5.1 Intervention du Bureau Van Dijk.

L'article 2 §2 de la loi du 11 avril 1994 organisant le vote automatisé dispose que tous les systèmes de vote et de dépouillement électronique ainsi que tout logiciel utilisé pour le comptage et la totalisation des résultats doivent être agréés par le Ministère de l'Intérieur,

Conformément à cet article, le 25 septembre 2002, le MI lançait un appel à candidatures en vue de désigner les organismes chargés de remettre un avis au Ministre sur les fournisseurs de systèmes de vote et de dépouillement électronique. Une société a répondu à cet appel et a été désignée: le Bureau Van Dijk.

Pour ce qui concerne notre mission, c-à-d les systèmes de vote et de dépouillement électronique, les fournisseurs ont reçu l' agrément du SPF Intérieur. Pour chacun d'eux, le Bureau Van Dijk a remis un avis.

Le Collège a reçu copie de ces avis au SPF Intérieur en présence des délégués du Bureau van DIJK et des fournisseurs.

Le travail effectué par le Bureau Van Dijk a permis de conforter le Collège dans les conclusions qu'il a rédigées tant lors des précédentes élections que pour les élections présentes.

Le Collège estime que cette nouvelle procédure d'agrément ne peut qu'augmenter la fiabilité des systèmes de votes et de dépouillement électronique. L' importance de l'avis émit mériterait une définition plus stricte des méthodes d'analyse et du temps à y consacrer.

5.2 Les améliorations au système de lecture optique (Favor)

Des améliorations avaient déjà été apportées en 2000 et de nouvelles ont encore été faites en 2003 :

- La ligne de coupe (sous les clocks) était trop finement imprimée pour permettre un réglage sur les machines de coupe. Les 2/10 de mm nécessaires (deux dixièmes de mm) ont été ajoutés.
- Les Bulletins de test en néerlandais reçoivent la mention OPVOLGERS au lieu de SUPPLEANTS (Aucune importance sur le lecteur mais plus cohérent).
- Les cases de tête de liste des suppléants ont été graphiquement améliorées (contour continu).
- Une indication de coupe de coin a été imprimée pour aider les opérateurs de la machine de coupe. Cette coupe de coin aide les opérateurs lors des élections à charger les Bulletins dans le bon sens dans le plateau d'entrée du lecteur. Rappelons que c'est l'origine des problèmes constatés en 1999 à Zonnebeke.

- Les clocks ont été réduites de 2/10 mm de hauteur (5,3 mm au lieu de 5,5 mm avec ligne de coupe incluse).
- Des améliorations ont été apportées en concertation continue avec l'imprimeur sur leur processus de fabrication industrielle des bulletins. (Meilleure qualité générale sans coût supplémentaire.)

5.3 Constatations à l'occasion des élections du 18 mai 2003

5.3.1 Fabrications des disquettes.

La fabrication des disquettes s'est déroulé dans un environnement central et bien sécurisé.

5.3.2 Démonstrations et tests effectués avant les élections

Afin de se familiariser avec les systèmes, le collège a effectué quelques essais sur les systèmes Digivote et Jites installés en version de démonstration par le SPF Intérieur. Une dizaine de votes ont été émis, visualisés ensuite et comparés avec les votes émis. Une totalisation a été également effectuée pour une situation fictive relative à 3 bureaux de vote avec le système Digivote.

L'équipement, prototype et définitif, destiné à compléter la configuration de base pour réaliser la fonction d'impression des suffrages a également été utilisé lors de démonstrations des systèmes Digivote et Jites.

Le système Favor n'a fait l'objet ni de démonstration ni de test.

5.3.3 La compilation de référence du 7 mai 2003

Objectif

- Compilation de la version définitive du code source des différents systèmes de vote dans un environnement sous contrôle du SPF Intérieur pour obtenir des codes exécutables de référence, la comparaison binaire de ceux-ci avec les codes exécutables utilisés le 18 mai 2000 ne pouvant montrer aucune différence;
- Obtention de ces codes source pour une analyse ultérieure.

Remarque

Lors des épreuves de compilations effectuées dans le cadre des contrôles d'élections précédentes, le collège avait exigé que ces compilations se fassent dans sur des PCs libres de toute configuration de départ. La raison principale était que le SPF Intérieur ne disposait pas d'environnement en propre dont il pouvait assurer au collège l'intégrité informatique (virus, piratage, etc.). Actuellement, le SPF dispose de tels environnements, un par système de vote. Les compilations ont donc été effectuées en partant de ces environnements de référence. Par ailleurs, le collège dispose encore des copies des environnements de compilation utilisés lors des contrôles des élections précédents. Ces copies pouvaient donc servir de point de comparaison par rapport aux environnements de développement de référence du SPF.

Constatations

- Digivote

Le CD-ROM contenant le code source du logiciel de vote a été extrait du coffre. Le collègue compile ensuite le code source reçu et prend une copie du disque dur. Cette copie est comparée aux copies d'environnement dont disposait le collègue. La comparaison révèle que l'environnement de référence utilisé pour la compilation est bien identique à la copie de l'environnement de développement faite à l'occasion du contrôle précédent, à l'exception de quelques bibliothèques nécessaires à l'affichage des logos des listes électorales.

- Jites

Mêmes constatations que pour Digivote.

- Fabricom

Le système d'exploitation, Microsoft Windows 98, et l'environnement de développement, Microsoft Visual Studio (C++) étaient déjà installés sur un PC de la société. La totalité du CD-ROM consigné dans le coffre et contenant le code source est copié sur le disque dur. Prend alors place une régénération dans tous les sous-répertoires concernés. Enfin, le collègue prend une copie intégrale de l'environnement de développement.

5.3.4 Analyse code de source

Est décrite ici l'analyse faite avant les élections. L'incident de Schaerbeek détaillé plus loin dans ce rapport, a bien entendu donné lieu à une étude plus détaillée de certaines parties du code.

Les remarques formulées à l'occasion des rapports précédents restent valables étant donné que les systèmes n'ont pas été fondamentalement modifiés. Les modifications essentielles apportées tant au système Digivote qu'au système Jites, sont:

- L'ajout de la fonction de ticketing
- La mise en oeuvre de l'AES (Advanced Encryption Standard), aussi appelé algorithme Rijndael

Bien que la disponibilité du code source offre en principe la possibilité de tester en profondeur le fonctionnement des systèmes, ceci n'a pu se faire vu les moyens et le temps dont disposait le collègue.

Il est par contre possible d'assurer que le logiciel ne contient pas de code permettant d'influencer frauduleusement le comptage. Le code source était d'ailleurs disponible avant que ne soient connus les numéros de liste; une fraude au niveau du code n'aurait donc été possible qu'au moyen de noms de listes et/ou de personnes (ce qui est facile à détecter).

Certaines remarques concernant le code source peuvent être faites au niveau de la qualité, et en particulier sur des caractéristiques telles que la lisibilité, la maintenance et la réutilisabilité.

5.3.4.1 Digivote

Il est rappelé que 'Digivote' est une collection de systèmes compatibles entre eux, comprenant

- Un logiciel pour le contrôle des machines à voter ;
- Un logiciel pour le contrôle de l'urne-pc;
- Un logiciel pour la totalisation dans les bureaux principaux de canton ;
- Un système pour la génération des disquettes "master" et "backup".

Les logiciels pour les machines à voter et pour les urnes-pc sont écrits en C++ et C (routines pour le cryptage et le décryptage) et sont intégralement compilés dans l'environnement de développement Borland C/C++ (version 3.1 pour MS-DOS).

Les logiciels de totalisation et de fabrication des disquettes sont écrits en Progress (version 6.2). Des "High-Level-Calls" sont entre autres utilisés pour le cryptage et le décryptage implémentés au moyen de routines C. Le "Microsoft C" (version 6.0 pour MS-DOS) est utilisé pour la compilation de ces routines et leur intégration dans l'environnement Progress.

Trois langages de programmation différents sont donc utilisés pour ce système.

Le code C++ est bien documenté, ce qui en accroît la lisibilité. Il est fait un usage intensif de variables globales, ce qui est désavantageux pour la maintenance du code et sa réutilisation ultérieure dans d'autres environnements.

Le code Progress est très peu documenté.

Le code source divulgué sur le site Web du SPF Intérieur est identique à celui utilisé lors de la compilation de référence.

5.3.4.2 Jites

Le logiciel pour le contrôle des machines à voter est développé en Microsoft C (version 6.0 pour MS-DOS). Le logiciel pour le contrôle de l'urne-PC est développé en Turbo C de Borland (version 2.0 pour MS-DOS).

Les systèmes pour la totalisation et la fabrication des disquettes sont développés en Clipper (version 5.0).

Le code source 'Jites' lui-même est peu documenté. Toutefois, une description détaillée du code source est disponible dans un document séparé.

Ici aussi, il est fait un usage intensif de variables globales. De plus, du code étroitement lié au matériel est utilisé au plus haut niveau (par exemple, gestion des portes dans le programme principal 'urne.c'). Ceci implique qu'un renouvellement du matériel peut éventuellement entraîner des modifications à plusieurs endroits dans le code. La réutilisabilité du code est par conséquent assez faible.

Le code source divulgué sur le site Web du SPF Intérieur est identique à celui utilisé lors de la compilation de référence.

5.3.4.3 Favor

Le système 'Favor' est un système de comptage optique de billets de votes. Il est développé en C++ (Visual Studio sous Windows 98) et fait usage de MFC (Microsoft Foundation Classes).

La documentation est pauvre.

L'algorithme 'Blowfish' est utilisé pour le cryptage et le décryptage. Contrairement aux systèmes décrits ci-dessus, le résultat du comptage n'est pas encrypté. Il est donc lisible. Toutefois, la signature numérique de ce fichier est cryptée. Le fichier peut donc être lu mais il ne peut être modifié sans que cela ne se remarque lors du contrôle du fichier 'signature'.

Ceci permet donc un contrôle aisé des résultats sans que la sécurité ne soit compromise.

Le code source divulgué sur le site Web du SPF Intérieur est identique à celui utilisé lors de la compilation de référence.

5.3.5 Constatations le jour des élections

5.3.5.1 Contrôle dans les bureaux de vote

Des contrôles ont été effectués dans les bureaux de vote suivants

Commune	N° de bureau	Système
Aalter	15	Digivote
Affligem	32	Digivote
Antween	25	Digivote
Awans	20	Jites
Berchem-Ste-Agathe	70	Digivote
Berlaare	16	Digivote
Boom	1	Digivote
De Panne	19	Digivote
Diepenbeek	68	Digivote
Durbuy	2 et 5	Jites
Frans-les-Anvain	2	Digivote
Ganshoren	54	Digivote
Genk	40	Digivote
Herentals	15	Digivote
Heverlee	31	Digivote
Jette	62	Digivote
Koekelber	84	Digivote
Koksijde	24 et 25	Digivote
Lebbeke	64	Digivote
Leuven	40	Digivote
Liège	30	Jites
Machelen	40	Digivote
Rocourt	137	Jites
Saint-Gilles	7	Digivote
Temat	112	Digivote
Turnhout	38	Digivote

Uccle	8	Digivote
Verlaine	4(ticketing)	Jites
Vilvoorde	6	Digivote
Fourons	3	Digivote
Waarschoot	5(ticketing)	Digivote
Zaventem	5	Digivote
Zomergem	7	Digivote
Zonhoven	84	Digivote

Des contrôles ont été effectués dans les bureaux de totalisation suivants:

Emplacement	système
Zonnebeke	Favor
Chimay	Favor
Lens	Totalisation Jites
Verlaine	Ticketing Jites
Waarschoot	Ticketing Digivote

5.3.5.2 Remarques particulières

Bureau de vote 8 à Uccle

Alors que l'expert du collège était présent, une machine à voter bloquée durant le vote d'une électrice a dû être réinitialisée par un membre des services communaux et le président du bureau.

Des files d'attente importantes ont été constatées à l'arrivée de l'expert du collège dès 09h00. Il a été constaté que de nombreux électeurs âgés ont requis l'aide du président de bureau pour utiliser le système pendant que l'expert du collège était présent. De telles interventions avaient pour conséquence d'allonger les délais nécessaires pour le vote des électeurs et contribuaient à l'augmentation des temps d'attente.

Bureau de vote 5 Waarschoot (Système Digivote avec ticketing)

De temps à autre, des techniciens devaient intervenir pour débloquer le défilement d'un ticket imprimé dans l'imprimante spéciale. Il faut donc remédier à ce mauvais fonctionnement.

Dans la matinée, des longues files d'attente s'étaient formées, avec une attente d'une demi-heure à trois quarts d'heure. Le président d'un bureau de dépouillement a signalé que les votes avaient duré beaucoup plus longtemps que lors des dernières élections. Il ne faut certainement pas en conclure que le ticketing en était la (seule) cause, car dans d'autres bureaux de vote (sans ticketing), il y avait des files d'attente comparables.

(voir Remarques générales)

Bureau de dépouillement Zonnebeke (lecture optique)

A l'arrivée dans l'hôtel de ville, le dépouillement avait déjà commencé à 15.55 heures. Le dépouillement, par une équipe expérimentée, s'est effectuée sans incidents et a pris fin vers 19.30 heures.

Il faut faire remarquer que les personnes effectuant le dépouillement avaient participé à des séances de préparation; le traitement s'est donc déroulé sans encombre. Il faut également mentionner que le processus de dépouillement n'est pas intégralement automatique, car il y a un tri ultérieur des cas douteux.

Le calibrage des systèmes s'est effectué par des techniciens de la firme Fabricom qui sont sur place pendant le dépouillement.

Bureau de totalisation de Lens

2 PC ont dû être écartés à cause de problèmes de démarrage (défectuosité du lecteur de disquettes) ; un jeu de disquettes a dû être re-généré sur place et 3 disquettes sur les 4 devant contenir le programme ont été identifiées comme défectueuses.

5.3.5.3 Remarques générales

Des copies du logiciel de vote ont été prises dans tous les bureaux. Ces copies ont été emportées pour analyse. Il en ressort que les exécutables utilisés le jour des élections sont strictement identiques (comparaison binaire) à ceux générés lors de la compilation de référence et dont le code source a été analysé par les experts.

De plus, un ou plusieurs votes de référence ont été émis dans chaque bureau de vote. Ces votes ont été visualisés sur des PCs différents de ceux utilisés pour l'émission des votes. Tous les votes de références ont été visualisés correctement.

Pour la première fois, le système ticketing a été testé. A Waarschoot il s'agissait du système Digivote, et à Verlaine du système Jites. Le système a fonctionné.

Des copies du logiciel de totalisation ont été prises dans tous les bureaux de totalisation. Ces copies ont été emportées pour analyse. Il en ressort que les exécutables des logiciels de totalisation utilisés le jour des élections sont strictement identiques (comparaison binaire) à ceux générés lors de la compilation de référence et dont le code source a été analysé par les experts.

Lors des contrôles effectués, il a été constaté que les files étaient visiblement plus longues que lors des élections précédentes. L'ajout d'écrans dans le processus de vote, ainsi que la communication claire de la possibilité d'un contrôle après le vote, sont des facteurs qui ont prolongé la durée des opérations de vote.

5.3.6 Contrôles effectués après les élections

Le test suivant a été effectué afin de montrer que le lecteur de cartes magnétiques ne modifie pas le contenu des cartes qui sont dans l'urne.

Une configuration matérielle Digivote similaire à celle utilisée dans les bureaux de vote est démarrée avec la même disquette que celle obtenue dans un bureau de Schaerbeek. Ensuite, les votes de références émis par les experts le jour des élections sont à nouveau visualisés. Il a pu être constaté que les votes concordaient.

La carte magnétique a ensuite été déposée dans l'urne, après quoi, elle a de nouveau été introduite dans la machine à voter et les votes émis ont à nouveau été visualisés. Le vote était

inchangé. Enfin, la carte magnétique a été mise dans l'urne une deuxième fois et à nouveau enregistrée. Le procédé a été répété avec différents votes émis au cours du test lui-même.

Dans le cas de chaque bureau de vote pour lequel les experts ont emporté une copie du logiciel de vote et des cartes magnétiques, les experts ont procédé à une reconstitution du bureau de vote: démarrage de l'urne et d'une machine à voter. Les votes enregistrés sur les cartes magnétiques ont été visualisés comme émis et les cartes introduites correctement dans les urnes.

Dans quelques cas, il a été tenté d'introduire une carte magnétique dans une urne correspondant à un autre bureau de vote. Dans chaque cas, la carte a été normalement refusée.

5.3.7 L'incident de Schaerbeek

Le collège a été prévenu d'un incident à Schaerbeek le 18 mai à 23h30. Il apparaissait dans le PV de totalisation, qu'un candidat d'une liste précise avait obtenu plus de voix de préférence que le nombre total de voix exprimées pour la liste de ce candidat.

Une enquête débuta le 19 mai en présence du président de canton, de représentants du SPF Intérieur, des sociétés Steria et Bureau Van Dijk et du collège d'experts.

Il apparut de l'analyse des disquettes des différents bureaux de vote que le problème se ramenait à un bureau de vote.

L'urne du bureau concerné a été demandée et il a été procédé à un recomptage des votes à partir des cartes magnétiques. Les disquettes contenant les nouveaux résultats ont été à nouveau totalisées avec les disquettes originales des autres bureaux de vote.

Le nouveau PV ne laissait plus apparaître l'erreur. La différence quant au nombre de voix de préférence était finalement de 4096.

Une réunion fut organisée le 22 mai, entre le collège d'experts et la société Steria en présence d'un représentant du SPF Intérieur. La conclusion commune atteinte était que l'erreur pouvait probablement être attribuée à une inversion spontanée d'une position binaire dans la mémoire vive du PC.

Le collège d'experts a effectué ce même jour une série de tests sur le PC du président du bureau de vote en question. Sur la base de ces tests, aucun problème au niveau du matériel n'a pu être constatée.

A l'issue des différents tests effectués les 22 et 23 mai (tests de la mémoire, nouvelle clôture du bureau, simulation d'opération de vote uniquement pour le candidat en question), l'incident n'a pu être reproduit.

5.3.7.1 Analyse technique du problème

Il ressort des constatations qu'il y avait un écart de 4096 voix de préférence pour un candidat. Un écart de 4096 peut être occasionné par une inversion de la 13ème position binaire du compteur.

5.3.7.2 Analyse détaillée du code source suite à l'incident de Schaerbeek.

Suite à l'étude de l'incident de Schaerbeek, il fut procédé à une analyse détaillée du code source en rapport avec l'incident. Il apparaît de cette analyse que:

- Toutes les données concernant le scrutin sont stockées dans une structure définie globalement dans la mémoire vive du PC du président;
- Cette structure globale est initialisée au démarrage du programme (ouverture du bureau de vote);
- Les différents compteurs (nombre de voix par liste, voix de préférence, ...) sont mis à 0 au démarrage du logiciel de l'urne.
- Les différents votes sont conservés en mémoire tampon pendant les opérations de vote (sous la forme de copies des contenus des cartes);
- Lors de la clôture du bureau de vote, les votes sont lus à partir de la mémoire tampon et les compteurs adéquats sont incrémentés;
- Le logiciel ne prévoit pas un double comptage ou une vérification croisée;
- Il n'y a dans le code source aucune instruction explicite qui aurait pu être à l'origine du phénomène.

Partant de l'hypothèse que l'erreur est due à une inversion spontanée de position binaire, il est de plus possible de conclure que celle-ci s'est produite entre le démarrage du logiciel de l'urne et la clôture du bureau de vote.

5.3.7.3 Conclusions du collège sur l'incident de Schaerbeek

Étant donné qu'aucune erreur n'a été trouvée dans le logiciel, et vu la structure interne du programme, le collège conclut que l'erreur a très probablement été occasionnée par une inversion spontanée et aléatoire d'une position binaire (ce phénomène est abondamment décrit dans la littérature spécialisée).

6 Conclusions

Dans les limites de la mission, des moyens et du temps disponibles, le collège conclut ce qui suit:

Lors de ces contrôles ponctuels dans les bureaux de vote le jour des élections, le collège n'a pas constaté de dysfonctionnements au niveau technique dans les systèmes de vote et de dépouillement automatisés. De même, lors de leurs analyses des codes sources, les experts n'ont relevé aucune anomalie dans les programmes.

L'incident d'un bureau de Schaerbeek est très vraisemblablement un incident isolé qui a été détecté d'une part par le bureau de canton de Schaerbeek dans son PV et d'autre part, par le SPF Intérieur au moyen de contrôles automatisés. Par ailleurs, cet incident n'a pu être reproduit. Il a pu y être remédié et il n'y a dès lors aucune incidence sur le résultat des élections.

Même si les systèmes ne sont pas parfaits, l'ensemble des contrôles effectués permet de s'assurer du bon fonctionnement global du déroulement du vote électronique. L'objectif visé, à savoir émettre les votes, les enregistrer, les visualiser et les compter selon les dispositions légales, a été atteint.

Concernant les écrans d'information complémentaires, le collège recommande de réévaluer les avantages (convivialité accrue) par rapport aux inconvénients (durée plus longue et files d'attente allongées).

L'expérience de " ticketing " s'est révélée satisfaisante en ce qu'elle a permis de montrer la fiabilité du vote électronique (émission et comptage des votes). Le dépouillement manuel des " tickets " est extrêmement difficile et fastidieux.

Le collège est convaincu que malgré les quelques problèmes mineurs rencontrés, le dépouillement électronique par lecture optique reste fiable et mûr.

Vu le caractère facultatif de la désignation des experts, le collège souhaite insister sur le fait que toutes les assemblées (en ce compris leurs administrations) doivent être conscientes de la nécessité et de l'importance du contrôle des systèmes de vote et de dépouillement automatisés qu'elles exercent par l'intermédiaire des experts qu'elles désignent.

Enfin, le collège remercie les fonctionnaires du Ministère de l'Intérieur pour leur bonne collaboration, ainsi que les représentants des différentes firmes avec qui ils ont été en contact. Le collège remercie également les présidents, assesseurs et témoins des bureaux de vote et de dépouillement automatisés pour leur coopération lors des contrôles pendant les élections.

E. Willems

F. Tomicki

M. Robert

W. Verhaest

J-P Gilson

R. Deboelpaep

B. Martens

CONFIDENTIEL

Bruxelles, le 4 juin 2003

Complément au rapport du collège d'experts chargé du contrôle du vote automatisé, concernant l'expérience « ticketing » à Waarschoot et Verlaine

Suite aux articles parus dans la presse au sujet des problèmes de comptage à Waarschoot, le collège a procédé à des contrôles complémentaires sur les résultats des expériences de ticketing à Verlaine et à Waarschoot. Ces contrôles ont été effectués sur la base d'informations supplémentaires fournies par le SPF Intérieur et des PV s mis à disposition par les assemblées.

Pour ces expériences de ticketing, le collège arrive aux conclusions additionnelles suivantes:

L'expérience, est concluante dans la mesure où, au niveau du vote, la concordance entre le vote visualisé à l'écran et imprimé a pu être établie dans l'isoloir.

L'expérience n'est pas concluante dans la mesure où la conception et la forme des tickets n'a pas permis d'effectuer le comptage manuel conformément aux prescriptions légales.

Le collège est d'avis que les résultats des opérations de dépouillement manuel des tickets ne peuvent être considérés comme fiables et que les résultats de la totalisation automatisée peuvent être considérés comme les plus fiables.

E. Willems

F. Tomicki

M. Robert

W. Verhaest

J-P Gilson

R. Deboelpaep

B. Martens