BRUSSELS HOOFDSTEDELIJK PARLEMENT

GEWONE ZITTING 2006-2007

18 OKTOBER 2006

VERSLAG

van het college van deskundigen belast met de controle op de geautomatiseerde stemmingen en stemopneming voor de gemeenteraadsverkiezingen in het Brussels Hoofdstedelijk Gewest

Gemeenteraadsverkiezingen van 8 oktober 2006

A-306/1 – 2006/2007

PARLEMENT DE LA REGION DE BRUXELLES-CAPITALE

SESSION ORDINAIRE 2006-2007

18 OCTOBRE 2006

RAPPORT

du collège des experts chargés du contrôle du système de vote et de dépouillement automatisés pour les élections communales en Région de Bruxelles-Capitale

Elections communales du 8 octobre 2006

Inhoudstafel

Table des matières

1. Samenstelling van het college

Op grond van artikel 5*bis*, § 5, van de ordonnantie tot wijziging van de wet van 11 april 1994 tot organisatie van de geautomatiseerde stemming werden er deskundigen aangewezen om tijdens de volgende verkiezingen van de leden van de gemeenteraden binnen het Brussels Hoofdstedelijk Gewest toe te zien op het gebruik en de goede werking van de geautomatiseerde stem- en telsystemen. Hun namen zijn de volgende :

Effectief :

De heer Jean-Marc Paul
De heer Geert Bryon
De heer Freddy Tomicki
De heer Theo D'Hondt

Plaatsvervangend :

Mevrouw Sophie Jonckheere
De heer Emmanuel Willems
De heer Johan Fabry
De heer Olivier Markowitch

Deze experten vormen het college van deskundigen.

Op grond van het derde lid van hetzelfde artikel 5*bis*, § 5, werden aangewezen als voorzitter de heer Jean-Marc Paul en als secretaris mevrouw Sophie Jonckheere.

2. De opdracht

2.1. De ordonnantie

Deze opdracht wordt geregeld door artikel 5bis van de Ordonnantie van 29 juni 2006 tot wijziging van de wet van 11 april 1994 tot organisatie van de geautomatiseerde stemming, vervangen bij de wet van 12 augustus 2000 en gewijzigd bij de wet van 11 maart 2003.

In het vet vindt u de onderdelen die betrekking hebben op de huidige missie.

« Art. 5*bis*. – § 1. – Bij de verkiezingen van de leden van de Kamer van Volksvertegenwoordigers en de Senaat, van het Europees Parlement en van de Gewest- en de Gemeenschapsraden, alsook van de raden voor maatschappelijk welzijn.

1. kunnen de Kamer van volksvertegenwoordigers, de Senaat en de Brusselse Hoofdstedelijke Raad elk twee effectieve deskundigen en twee plaatsvervangende deskundigen aanwijzen;

2. kunnen de Vlaamse Raad, de Waalse Gewestraad en de Raad van de Duitstalige Gemeenschap elk één effectieve

1. Composition du collège

En application de l'article 5*bis*, § 5, de l'ordonnance du 29 juin 2006 modifiant 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 membres des conseils communaux en Région de Bruxelles-Capitale, les experts dont les noms suivent :

Effectifs :

Monsieur Jean-Marc Paul
Monsieur Geert Bryon
Monsieur Freddy Tomicki
Monsieur Theo D'Hondt

Suppléants :

Madame Sophie Jonckheere
Monsieur Emmanuel Willems
Monsieur Johan Fabry
Monsieur Olivier Markowitch

Ces experts forment le collège d'experts.

En application de l'alinéa 3 du même article 5*bis*, § 5, ont été désignés comme président M. Jean-Marc Paul et comme secrétaire Mme Sophie Jonckheere.

2. La mission

2.1. L'ordonnance

Cette mission est réglée par l'article 5*bis* de l'ordonnance du 29 juin 2006 modifiant la loi du 11 avril 1994 organisant le vote automatisé, remplacé par la loi du 12 août 2000 et modifié par la loi du 11 mars 2003.

Les parties concernant l'actuelle mission sont indiquées en caractères gras.

« Art. 5*bis*. – § 1er. – Lors de l'Election 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 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

deskundige en één plaatsvervangende deskundige aanwijzen.

Deze aanwijzingen kunnen zowel bij de volledige vernieuwing van elke vergadering gebeuren als bij een herverkiezing die georganiseerd wordt naar aanleiding van de vernietiging van een verkiezing, evenals bij een verkiezing ingevolge een vacature waarin niet kan worden voorzien door het aanstellen van een opvolger.

De personen bedoeld in het eerste lid vormen het college van deskundigen. Zij wijzen een voorzitter en een secretaris aan in hun midden.

§ 2. – Tijdens de verkiezingen zien de deskundigen toe op het gebruik en de goede werking van alle geautomatiseerde stem- en stemopnemingssystemen evenals op de procedures betreffende de aanmaak, de verspreiding en het gebruik van apparatuur, programmatuur en de elektronische informatiedragers. De deskundigen ontvangen van het ministerie van Binnenlandse Zaken het materiaal, alsook alle gegevens, inlichtingen en informatie die nodig zijn voor het uitoefenen van controle op de geautomatiseerde stem- en stemopnemingssystemen.

Zij kunnen in het bijzonder de betrouwbaarheid controleren van de software in de stemmachines, de correcte omschrijving van de uitgebrachte stemmen op de magneetkaart, de correcte omschrijving door de elektronische stembus van de uitgebrachte stemmen op de geheugendrager van het stembureau, de correcte registratie van de geheugendrager van het stembureau op de geheugendrager bestemd voor het optellen van de stemmen, de totalisering van de uitgebrachte stemmen, de optische lezing van de uitgebrachte stemmen en het controlesysteem van de geautomatiseerde stemming voor het afdrukken van de uitgebrachte stemmen op papier.

Zij verrichten de controle vanaf de 40e dag voor de verkiezing, op de verkiezingsdag zelf en hierna tot de indiening van het verslag bedoeld in § 3.

§ 3. – Uiterlijk vijftien dagen na de sluiting van de stemming en in ieder geval voor de geldigverklaring van de verkiezingen wat de Kamer van volksvertegenwoordigers en de Senaat, de Gewest- en de Gemeenschapsraden en het Europees Parlement betreft, bezorgen de deskundigen een verslag aan de minister van Binnenlandse Zaken, aan de federale wetgevende assemblees, de Gewest- en Gemeenschapsraden. Uiterlijk tien dagen na de sluiting van de stemming en in ieder geval voor de geldigheidsverklaring van de verkiezingen wat de raden voor maatschappelijk welzijn betreft, bezorgen zij een verslag aan de minister van Binnenlandse Zaken en aan de federale wetgevende assemblees.

Hun verslag kan in het bijzonder aanbevelingen bevatten in verband met het materiaal en de software die werden gebruikt.

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 avent la validation des élections pour ce qui concerne les conseils 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. – De deskundigen zijn tot geheimhouding verplicht. Elke schending van de geheimhoudingsplicht wordt bestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 5. – Bij de verkiezingen van de leden van de gemeenteraden binnen het Brussels Hoofdstedelijk Gewest, wijst het Parlement van het Brussels Hoofdstedelijk Gewest vier effectieve deskundigen en vier plaatsvervangende deskundigen aan.

Deze aanwijzingen kunnen zowel bij de volledige vernieuwing van de gemeenteraden gebeuren als bij een herverkiezing die georganiseerd wordt naar aanleiding van de vernietiging van een verkiezing, evenals bij een verkiezing ingevolge een vacature waarin niet kan worden voorzien door het aanstellen van een opvolger.

De personen bedoeld in het eerste lid vormen het college van deskundigen voor de gemeenteraadsverkiezingen.

De plaatsvervangende deskundigen verlenen bijstand aan de effectieve leden bij de uitvoering van de in § 6 bedoelde opdrachten of vervangen hen in geval van verhindering. Dit college wijst een voorzitter en een secretaris aan in hun midden.

§ 6. – Tijdens de verkiezingen zien de deskundigen toe op het gebruik en de goede werking van alle geautomatiseerde stem- en stemopnemingssystemen evenals op de procedures betreffende de aanmaak, de verspreiding en het gebruik van apparatuur, programmatuur en de elektronische informatiedragers. De deskundigen ontvangen van het ministerie van het Brussels Hoofdstedelijk Gewest het materiaal, alsook alle gegevens, inlichtingen en informatie die nodig zijn voor het uitoefenen van controle op de geautomatiseerde stem- en stemopnemingssystemen.

Zij kunnen in het bijzonder de betrouwbaarheid controleren van de software in de stemmachines, de correcte overschrijving van de uitgebrachte stemmen op de magneetkaart, de correcte overschrijving door de elektronische stembus van de uitgebrachte stemmen op de geheugendrager van het stembureau, de correcte registratie van de geheugendrager van het stembureau op de geheugendrager bestemd voor het opstellen van de stemmen, de totalisering van de uitgebrachte stemmen, de optische lezing van de uitgebrachte stemmen en het controlesysteem van de geautomatiseerde stemming voor het afdrukken van de uitgebrachte stemmen op papier.

Zij verrichten de controle vanaf de 40e dag voor de verkiezing, op de verkiezingsdag zelf en hierna tot de indiening van het verslag bedoeld in § 7.

§ 7. – Uiterlijk tien dagen na de sluiting van de stemming en in ieder geval voor de geldigheidsverklaring

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

§ 5. – Lors de l'élection des membres des conseils communaux en Région de Bruxelles-Capitale, le Parlement de la Région de Bruxelles-Capitale désigne quatre experts effectifs et quatre experts suppléants.

Ces désignations peuvent être effectuées tant lors du renouvellement complet des conseils communaux 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 pour les élections communales.

Les experts suppléants apportent leur assistance aux membres effectifs dans l'exécution des missions mentionnées au § 6 ou les remplacent en cas d'empêchement. Ce collège désigne en son sein un président et un secrétaire.

§ 6. – 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 la Région dze Bruxelles-Capitale 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 § 7.

§ 7. – Au plus tard dix jours après la clôture des scrutins et en tout état de cause avant la validation des élec-

van de verkiezingen bezorgen de deskundigen aangeduid in uitvoering van § 5 een verslag aan de regering en aan het Parlement van het Brussels Hoofdstedelijk Gewest. Dit verslag kan aanbevelingen bevatten in verband met het materiaal en de software die werden gebruikt.

§ 8. – Deze deskundigen zijn tot geheimhouding verplicht. Elke schending van de geheimhoudingsplicht wordt bestraft overeenkomstig artikel 458 van het Strafwetboek. »

2.2. De taak van de deskundigen

Hoewel de verschillende colleges van deskundigen dit punt al hebben aangebracht naar aanleiding van de vorige verkiezingen, is de rol van de plaatsvervangende leden, bepaald bij artikel 5*bis*, § 5, nog altijd niet duidelijk omschreven. De laatste zin van genoemde paragraaf stelt dat de plaatsvervangende deskundigen bijstand verlenen aan de effectieve leden bij de uitvoering van hun controle opdrachten. Het college heeft, opnieuw, gekozen voor de ruimste interpretatie en beschouwt de plaatsvervangende leden als volledig gerechtigde leden van het college, met dezelfde controlerechten.

3. Werkprincipes van de geautomatiseerde stemming

Een geautomatiseerd stemsysteem bestaat uit verschillende componenten waarvan de stemmachine in het kieshokje, het meest zichtbare voor de kiezer, slechts één onderdeel is. Er zijn immers verschillende fasen in het verkiezingsproces en met elke fase correspondeert een welbepaald deelsysteem van het geautomatiseerd stemsysteem. Eerst en vooral is er de voorbereiding in de weken voor de verkiezingen. Hierin spelen zowel de constructeur van het geautomatiseerd stemsysteem als het MBHG (Ministerie van het Brussels Hoofdstedelijk Gewest) een rol. Op de dag van de verkiezingen is er de procedure in het stembureau. Ten slotte speelt zich op de avond van de verkiezingen nog een derde fase van de geautomatiseerde stemming af in de hoofdbureaus waar de totalisatie van de stemmen plaatsvindt. Er zijn geen stemopnemingsbureaus.

De procedure in het stembureau en het deelsysteem dat met deze procedure correspondeert, bepaalt grotendeels het verloop van de eerste en de derde fase (resp. de voorbereiding en de totalisatie). We beginnen dit overzicht dan ook in het stembureau zelf. Nadien komt de totalisatie op het niveau van de gemeente aan bod en ten slotte de voorbereiding van de verkiezingen in het MBHG.

Er bestaan in feite twee stemsystemen : het Digivote en het Jites systeem, zoals tijdens de vorige verkiezingen.

tions, les experts désignés en vertu du § 5 doivent remettre un rapport au Gouvernement et au Parlement de la Région de Bruxelles-Capitale. Ce rapport peut comprendre des recommandations relatives au matériel et aux logiciels utilisés.

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

2.2. Rôle des experts

Bien que le collège d'experts ait soulevé ce point à l'occasion du contrôle effectué lors des précédentes élections, le rôle des membres suppléant prévus par l'article 5*bis*, § 5, n'est toujours pas clairement défini. La dernière phrase de ce paragraphe dispose que les experts suppléants apportent leur assistance aux membres effectifs dans l'exécution des missions. 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 même pouvoirs de contrôle.

3. Principes de fonctionnement du 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 MRBC (Ministère de la Région de Bruxelles-Capitale) jouent un rôle. Le jour des élections, il y a la procédure dans le bureaux de vote. Le soir des élections enfin, on assiste à une troisième phase du vote automatisé dans le bureaux principaux où les votes sont totalisés. Il n'y a pas de bureau de dépouillement.

La procédure dans le bureau de vote et la partie du système qui correspond à cette procédure déterminant dans une large mesure le déroulement des première et troisième phases (c'est-à-dire la préparation et la totalisation). Nous commençons dès lors cet aperçu dans le bureau de vote même. Nous abordons ensuite la totalisation au niveau de la commune, et enfin la préparation des élections au MRBC.

Il existe en fait deux systèmes de vote : le système Digivote et le système Jites, comme lors des élections précédentes.

De verschillen situeren zich vooral op het gebied van het gebruikte materiaal en van de gebruikersinterface (de kiezer of de voorzitter van het stem- of totalisatiebureau).

In tegenstelling met vorige verkiezingen waar beide types hardware over specifieke software beschikten, is er voor de gemeenteraadsverkiezingen van 2006 in Brussel slechts één software die rekening houdt met de verschillen tussen beide types hardware. De software werd geschreven door de firma Stesud (die het Jites systeem heeft ontworpen) na een aanbesteding die volgde op een gemeenschappelijke oproep van het Brussels Hoofdstedelijk Gewest en van het Waalse Gewest.

3.1. Het stembureau

3.1.1. De procedure

De procedure in het stembureau bij een geautomatiseerde stemming is sterk gelijkaardig aan deze bij de traditionele stemming. In de stembureaus met geautomatiseerde stemming zijn er echter geen stembiljetten meer. De rol van de stembiljetten wordt overgenomen door magneetkaarten. Elk stemhokje van een stembureau bevat een stemmachine. Iedere stemmachine is uitgerust met een beeldscherm, een eenheid voor het lezen en het registreren van magneetkaarten en een lichtpen. Ook de traditionele stembus is vervangen door een elektronische urne. In vergelijking met de stemming op papier zorgt de urne-PC voor de elektronische uitgifte van de stemformulieren en het opslaan van deze formulieren in de urne.

3.1.1.1. Opening van het stembureau

De voorzitter van het stembureau ontvangt de dagen voor de verkiezingen een verzegelde omslag met diskettes (een master en meerdere back-ups die de taak van de eerste overneemt bij defect) die dienen om de stemmachines en de urne te activeren en een aparte verzegelde omslag met het paswoord voor het gebruik van deze diskettes. Elk stembureau heeft een verschillend paswoord. De verzegelde omslagen mogen slechts worden geopend in aanwezigheid van de leden van het bureau op de dag van de verkiezingen. De stemmachines zelf en de elektronische urne worden de week voor de verkiezingen door de gemeente geïnstalleerd. Zonder de vermelde diskettes (die de software van het stemsysteem bevat) kan deze apparatuur echter niet worden geactiveerd.

Bij de opening van het stembureau controleert de voorzitter of de bak van de urne leeg is, waarna de urne wordt afgesloten en verzegeld. Daarna start hij met behulp van de geleverde master-diskette en zijn paswoord, de elektronische urne en de stemmachines op. De master-diskette blijft voor het verdere verloop van de stemming in de urne zitten en wordt gebruikt om er de stemmen op te registreren.

Les différences se situent essentiellement au niveau du matériel utilisé et aux interfaces présentées aux utilisateurs (l'électeur ou le président du bureau de vote ou de totalisation).

Contrairement aux élections précédentes où chaque matériel disposait de son propre logiciel, il n'y a, pour les élections communales de 2006 à Bruxelles, qu'un seul logiciel qui tient compte des différences entre les deux types de matériels. Ce logiciel a été développé par la société Stesud (qui a conçu la système Jites) après adjudication du marché suite à l'appel d'offre lancé en commun par la Région bruxelloise et la Région wallonne.

3.1. Le bureau de vote

3.1.1. La procédure

Lors d'un vote automatisé, la procédure dans le bureau de vote est fort semblable à celle du vote traditionnel. Mais dans les bureaux de vote automatisé, il n'y a plus de bulletins de vote. Les bulletins de vote sont remplacés par ces cartes magnétiques. Chaque isoloir d'un bureau de vote est pourvu d'une machine à voter. Chaque machine à voter est équipée d'un écran de visualisation, d'un lecteur-enregistreur de cartes magnétiques et d'un crayon optique. L'urne traditionnelle est aussi remplacée par une urne électronique. Par comparaison avec le vote sur papier, l'urne-PC délivre électroniquement les bulletins de vote et les stocks.

3.1.1.1. Ouverture du bureau de vote

Le président du bureau de vote reçoit dans les jours précédant les élections une enveloppe scellée avec les disquettes (une disquette maîtresse et plusieurs disquettes de sauvegarde qui reprennent la tâche de la première en cas de défectuosité) qui servent à activer les machines de vote et l'urne, et une enveloppe scellée distincte contenant le mot de passe pour utiliser ces disquettes. Le mot de passe diffère pour chaque bureau de vote. Les enveloppes scellées ne peuvent être ouvertes que le jour des élections en présence des membres du bureau. Les machines à voter mêmes et l'urne électronique sont installées par la commune la semaine qui précède les élections. Sans les disquettes mentionnées (qui contiennent le logiciel du système de vote), il est impossible d'activer ces machines.

Lors de l'ouverture du bureau de vote, le président contrôle que le bac de l'urne est vide, après quoi l'urne est fermée et scellée. Ensuite, il active l'urne électronique et les machines à voter à l'aide de la disquette maîtresse et du mot de passe fournis. La disquette maîtresse reste dans l'urne pour le déroulement ultérieur du vote et set à l'enregistrement des votes.

3.1.1.2 Het verloop van de stemming

Een kiezer biedt zich aan en legt zijn oproepingsbrief en identiteitskaart voor aan de voorzitter. De voorzitter neemt een nieuwe magneetkaart, initialiseert deze en overhandigt de kaart aan de kiezer. Elke magneetkaart kan slechts éénmaal worden aangewend voor de kiesverrichting. Voor het uitbrengen van de stem, dient elke magneetkaart immers te worden geïnitialiseerd (gebruiksklaar gemaakt) opdat ze enkel in dat bureau kan gebruikt worden. De initialisatie gebeurt met behulp van een magneetkaartschrijver in de urne-PC.

De kiezer neemt de geïnitialiseerde magneetkaart mee naar het stemhokje en stopt deze in de gleuf van de stemmachine. Elke foutieve of niet geïnitialiseerde kaart wordt geweigerd.

Het scherm geeft aanwijzingen tijdens de hele stemverrichting. Er wordt aan de kiezer gevraagd om zijn stem uit te brengen (blanco, lijststem, één of meerdere kandidaten van dezelfde lijst). Nadat de kiezer zijn stem heeft uitgebracht met behulp van de lichtpen, moet hij zijn keuze bevestigen. Vanaf dat moment is de stem definitief. Zolang er geen bevestiging is, kan de kiezer zijn stem annuleren en opnieuw beginnen. Als hij zijn kaart teruggeeft zonder gestemd te hebben, wordt zijn stem ook beschouwd als een blanco stem (onthouding). Ongeldig stemmen door te panacheren wordt niet toegelaten door het systeem.

Na bevestiging van de stemming, wordt de kaart door de stemmachine uitgeworpen. De kiezer kan dan zijn kaart terug in de stemmachine stoppen. De machine detecteert dat er al op die kaart is gestemd. Zij stelt dan de kiezer voor om de stem die op de kaart staat terug te bekijken.

Nadat de kiezer heeft gestemd, overhandigt hij zijn magnetische kaart aan de voorzitter die nagaat of er geen zichtbaar merkteken op de kaart staat. De kaart wordt in de gleuf van de elektronische urne gestoken (waarin zich eveneens een magneetkaartlezer bevindt) en de stem wordt geregistreerd.

In het geval van de Digivote hardware, wordt de stem op diskette en in het geheugen (ramdisk) geschreven. In het geval van Jites, wordt de stem in een EEPROM geschreven en in het geheugen (ramdisk).

3.1.1.3 Sluiten van het stembureau

Op het einde van de stemming sluit de voorzitter de stemoperaties af. Vanaf nu kan geen enkele stem meer worden geregistreerd met de elektronische urne. Alle apparatuur wordt afgezet. De diskette met de resultaten (en twee back-ups) worden in een verzegelde omslag gestopt en door de voorzitter naar het hoofdbureau gebracht voor totalisatie. De magneetkaarten blijven in de verzegelde elektronische urne tot na de geldigverklaring van de verkiezingen, tenzij een hertelling door het hoofdbureau zou worden gevraagd.

3.1.1.2. Le déroulement du vote

Un électeur se présente et remet sa convocation et sa carte d'identité au président. Le président prend une nouvelle carte magnétique, l'initialise et la remet à l'électeur. Chaque carte magnétique ne peut être utilisée qu'une seule fois pour l'opération de vote. Avant le vote, chaque carte magnétique doit en effet être initialisée (rendue opérationnelle) afin de ne pouvoir être utilisée que pour le vote dans le bureau. L'initialisation se fait dans l'urne-PC au moyen d'un lecteur de carte magnétique.

L'électeur emporte la carte magnétique initialisée dans l'isoloir et l'introduit dans la fente de la machine à voter. Toute carte mal initialisée ou non initialisée est refusée.

L'écran affiche des indications pendant toute l'opération de vote. Il est demandé à l'électeur d'exprimer son vote (vote blanc, vote en tête de liste, un ou plusieurs candidats de la même liste). Lorsque l'électeur a exprimé son vote avec le crayon optique, il doit le confirmer. A partir de ce moment, le vote est définitif. Tant qu'il n'est pas confirmé, l'électeur peut annuler son vote et recommencer. S'il remet sa carte sans avoir voté, sa voix est considérée comme un vote blanc (abstention). Le système ne permet pas de voter nul en « panachant ».

Après confirmation du vote, la machine à voter éjecte la carte. L'électeur peut alors réintroduire sa carte dans la machine à voter, et celle-ci détecte alors qu'un vote est présent sur la carte. Elle propose alors à l'électeur de visualiser le vote enregistré sur la carte.

Après avoir voté, l'électeur remet sa carte magnétique au président qui vérifie que la carte ne comporte aucune marque visible. La carte est introduite dans la fente de l'urne électronique (qui comporte également un lecteur de cartes magnétiques) et le vote est enregistré.

Dans le cas du matériel Digivote, le vote est enregistré sur disquette et en mémoire (ramdisk). Dans le cas du matériel Jites, le vote est enregistré dans une EEPROM et en mémoire (ramdisk).

3.1.1.3. Fermeture du bureau de vote

A la fin du vote, le président clôt les opérations de vote. A partir de cet instant, l'urne électronique ne peut plus enregistrer aucun vote. Toutes les machines sont éteintes. La disquette avec les résultats (et deux copies de sauvegarde) sont mises dans une enveloppe scellée et sont amenées par le président au bureau principal pour la totalisation. Les cartes magnétiques restent dans l'urne électronique scellée jusqu'à la validation des élections, à moins d'une demande de recomptage du bureau principal.

3.1.2 De hardware

3.1.2.1. De stemmachines

3.1.2.1.1. De Digivote stemmachine

De stemmachine is het toestel dat zich in het stemhokje bevindt. De hardware van een Digivote-stemmachine is gebaseerd op een standaard PC type x86 met 2 seriële poorten, 1 parallelle poort, 1 diskettelezer 3.5" 1.44 MB, een lichtpen, een magneetkaartlezer en -schrijver, en een scherm.

Aan de achterkant van de PC is een alarmdoosje bevestigd (zichtbaar voor de voorzitter) met een rood en een groen lampje en een reset-knop.

Het scherm is een 14" scherm gebruikt in monochroom mode, hoewel de werking van het stemsysteem onafhankelijk is van het type scherm.

De kiezer heeft enkel toegang tot de magneetkaartlezer, de lichtpen en het scherm. De diskettelezer, de stroomschakelaar en de reset-knop bevinden zich achter een gesloten deurtje. Het alarmdoosje bevindt zich buiten het stemhokje.

Een stemmachine bevat geen toetsenbord en normaal gezien ook geen harde schijf. Toch kunnen de gemeentebesturen, die eigenaar zijn van de apparatuur, tussen de verkiezingen, beslissen om de stemmachines te gebruiken als burotica PC's. Dit vraagt een wijziging van de standaard hardwareconfiguratie, in casu het toevoegen van een harde schijf. Bij het gebruik als stemmachine moet deze harde schijf echter worden gedeactiveerd. Hiervoor bestaat een testdiskette die de dag voor de verkiezingen, na de installatie van de apparatuur, nagaat of de machine correct is geconfigureerd. In buroticaconfiguraties wordt daarbij de harde schijf op BIOS-niveau gedeactiveerd.

3.1.2.1.2 De Jites-stemmachine

De stemmachine Jites is, wat zijn componenten betreft, een standaard PC met een speciaal omhulsel. Alle randapparatuur en aansluitingen bevinden zich achteraan (stroomaansluiting, toetsenbordaansluiting, optische leespenaansluiting, een parallelle poort, twee seriële poorten, schermaansluiting, diskettesation, alarmlichtjes, drukknop voor het uitwerpen van de magneetkaart). Enkel de magneetkaartlezer is vooraan beschikbaar en is dus de enige component van de PC waartoe de kiezer toegang heeft.

De stemmachine heeft een PC-architectuur, dit wil zeggen zij heeft een moederbord met ene processor van het type x86. De enige randapparatuur voor gegevensopslag is het diskettestation, er is geen harde schijf, noch CD lezer. Het scherm is een 14" scherm dat in monochroommode gebruikt wordt.

3.1.2. Le matériel

3.1.2.1. Les machines à voter

3.1.2.1.1. La machine à voter Digivote

La machine à voter est l'appareil installé dans l'isoloir. Le matériel d'une machine à voter Digivote est constitué d'un PC standard (type x86) avec 2 ports sériels, 1 port parallèle, 1 lecteur de disquette 3.5" 1.44 MB, un crayon optique, un lecteur-enregistreur de cartes magnétiques et un écran.

Une boîte d'alarme (que le président peut voir) est fixée à l'arrière du PC avec un voyant rouge et un voyant vert ainsi qu'un bouton de remise à zéro.

L'écran est un écran 14" utilisé en mode monochrome, mais le fonctionnement du système de vote est indépendant du type d'écran.

L'électeur a uniquement accès au lecteur de cartes magnétiques, au crayon optique et à l'écran. Le lecteur de disquette, le commutateur de l'alimentation électrique et le bouton de remise à zéro se trouvent derrière une petite porte fermée. Le boîtier d'alarme se trouve hors de l'isoloir.

Une machine à voter n'a ni clavier ni, normalement, de disque dur. Les administrations communales, qui sont propriétaires du système, peuvent néanmoins décider d'utiliser, entre les élections, les machines à voter comme PC de bureautique. Il faut alors modifier la configuration du matériel standard, à savoir en ajoutant un disque dur. Lorsque l'appareil est utilisé comme machine à voter, il faut toutefois désactiver le disque dur. Il existe à cet effet une disquette de test qui vérifie la veille des élections, après l'installation du système, que la machine a été configurée correctement. Dans des configurations de bureautique, le disque dur se trouve alors désactivé au niveau BIOS.

3.1.2.1.2. La machine à voter Jites

La machine à voter Jites est un PC standard (quant à ses composants) avec un boîtier particulier. Tous les périphériques et prises sont situés sur la face arrière (prise pour le raccordement au réseau électrique, prise pour le clavier, prise pour le crayon optique, un port parallèle, deux ports sériels, prise pour écran, lecteur de disquette, lumières d'alarme, bouton d'éjection de la carte magnétique). Seul le lecteur de carte magnétique est disponible sur la face avant et est donc le seul composant du PC auquel l'électeur a accès.

La machine à voter est dotée d'une architecture de type PC, c'est-à-dire qu'elle est dotée d'une carte-mère équipée d'un processeur de type x86. Le seul périphérique de stockage est le lecteur de disquette : il n'y a ni disque dur, ni lecteur de CD. L'écran est un écran 14" utilisé en mode monochrome.

3.1.2.2 De urnen

3.1.2.2.1 De Digivote urne

De urne-PC is het toestel dat voorbehouden is voor de voorzitter van het stembureau. In het stembureau is dit het enige toestel met een klavier. Het is eveneens op dit toestel dat de elektronische urne is aangesloten. Per stembureau is er slechts één urne-PC.

Ook dit is een standaard-PC voorzien van een magneetkaartlezer en -schrijver, echter zonder lichtpen maar wel met een klavier. De PC is via een seriële kabel verbonden met een magneetkaartbak (urne). De magneetkaartbak bestaat uit een metalen bak, met een deksel met magneetkaartlezer en een voeding.

De analogie tussen de hardware van een stemmachine en de urne-PC laat toe, bij defect van de urne-PC, een stemmachine op te waarderen tot urne-PC door de lichtpen van de stemmachine te verwijderen en de magneetkaartbak en een klavier te bevestigen.

Bij technische problemen kan de voorzitter steeds een beroep doen op de technische assistentie georganiseerd door de leverancier van de apparatuur.

3.1.2.2.2 De Jites urne

De urne is volledig verschillend van deze bij het Digivote systeem. Het is een grote metalen doos die tijdens de verkiezingen wordt verzegeld en waarbij het deksel een PC bevat die de werking van de urne beheert. Deze metalen doos heeft een ingebouwde magneetkaartlezer die zal gebruikt worden bij het deponeren van de kaarten in de urne en een extern leesstation voor het initialiseren van de magneetkaarten.

De PC bevat een moederbord met een processor van het type x86, een diskettestation, een numeriek toetsenbord (stijl Bancontact), een liquid cristal scherm van 2 lijnen van 20 karakters, controle lampjes, batterijcompartiment, een EEPROM-schrijver (= permanent geheugen), een stroomaansluiting, een aansluiting voor een extern scherm, en een aansluiting voor een extern leesstation voor magneetkaarten.

3.1.3 Werking van de systemen

3.1.3.1 De stemmachine

Een stemmachine biedt de volgende basisfunctionaliteiten :

– het inlezen van de magneetkaart van de kiezer

3.1.2.2. Les urnes

3.1.2.2.1. L'urne Digivote

L'urne-PC est l'appareil réservé au président du bureau de vote. C'est la seule machine, dans le bureau de vote, qui dispose d'un clavier. C'est également à cette machine qu'est reliée l'urne électronique. Il n'y a qu'une seule urne-PC par bureau de vote.

Il s'agit aussi d'un PC standard équipé d'un lecteur-enregistreur de cartes magnétiques, sans crayon optique mais avec clavier. Le PC est relié par un câble série à un bac à cartes magnétiques (l'urne). Le bac à cartes magnétiques se compose d'un bac en métal avec un couvercle avec un lecteur de cartes magnétiques et une alimentation électrique.

Comme le matériel d'une machine à voter ressemble à celui de l'urne-PC, il est possible, en cas de panne de l'urne-PC, de transformer une machine à voter en urne-PC en enlevant le crayon optique de la machine à voter et en y fixant un bac à cartes magnétiques et une clavier.

En cas de problèmes techniques, le président peut toujours faire appel à l'assistance technique organisée par le fournisseur de l'appareil.

3.1.2.2.2. L'urne Jites

L'urne est un appareil tout à fait différent de celle du système Digivote. Il s'agit d'une grande boîte métallique qui est scellée lors des élections et dont le couvercle renferme un PC qui sert à la gestion de l'urne. Cette boîte métallique est dotée d'un lecteur intégré de cartes magnétiques qui sera utilisé pour le dépôt des cartes dans l'urne et d'un lecteur externe qui sera utilisé pour l'utilisation des cartes magnétiques.

Le PC comprend une carte-mère dotée d'un processeur de type x86, d'un lecteur de disquettes, d'un clavier sous la forme d'un pavé numérique (style clavier Bancontact), d'un écran à cristaux liquides de 2 lignes de 20 caractères, de lampes de contrôle, d'un compartiment pour batteries, d'un graveur d'EEPROM (c'est-à-dire mémoire permanente), d'une prise pour l'alimentation électrique, d'une prise pour le raccordement d'un écran externe et d'une prise pour le raccordement du lecteur de cartes magnétiques externe.

3.1.3. Fonctionnement des systèmes

3.1.3.1. La machine à voter

Une machine à voter offre les fonctions de base suivantes :

– elle lit la carte magnétique de l'électeur

– het begeleiden van de kiezer via berichten op het scherm

– het vertonen van de elektronische kiesbrief

– het aanvaarden en geldig verklaren van de door de kiezer uitgebrachte stem

– het wegschrijven van de stem op de magneetkaart

– het herbekijken van de stem die hij heeft uitgebracht.

De master-diskette uit de verzegelde envelop die de voorzitter op de dag van de verkiezingen mag openen, is een systeem opstartdiskette (DOS bootable) en wordt gebruikt om de stemmachines op te starten. Het is dezelfde diskette die vooraf werd gebruikt om de urne-PC te activeren (zie verder). De software detecteert immers automatisch of het om een stemmachine of een urne-PC gaat en van welk type (Digivote of Jites).

Na het opstarten, zal de stemmachine een numeriek toetsenbord op het scherm laten verschijnen. Er wordt aan de voorzitter gevraagd om zijn paswoord in te geven. De stemmachine is dan operationeel.

Voor een stemmachine begint een stemming met de invoer van een gevalideerde magneetkaart. Het stemprogramma controleert of :

– de kaart correct in de lezer werd gestopt, zoniet wordt de gebruiker hierop attent gemaakt

– de kaartinhoud leesbaar is, zoniet wordt de kiezer gevraagd om de voorzitter op de hoogte te brengen

– de kaart gevalideerd is voor dit stembureau zoniet wordt ook in dit geval aan de kiezer gevraagd om de voorzitter op de hoogte te brengen.

Als de kaart correct is ingebracht kan de kiezer zijn stem uitbrengen, met behulp van een lichtpen. De selectie van een element op het scherm gebeurt door de lichtpen loodrecht op de zone te plaatsen die de keuze aangeeft en te drukken op het scherm. Buiten deze actieve zones wordt elke druk op de pen genegeerd.

Na de stemming registreert de stemmachine de informatie op de magneetkaart voor elke verkiezing waarvoor de kiezer een stem heeft uitgebracht.

Daarnaast wordt nog een testbit weggeschreven die aangeeft dat er met deze kaart effectief is gestemd en een controlegetal die de integriteit van de stem moet garanderen. Dit controlegetal zal de elektronische urne toelaten te verifiëren dat de stem geregistreerd op de magneetkaart effectief een correcte stem is, uitgebracht met een stemmachine van het stembureau op de dag van de verkiezingen.

– elle guide l'électeur par des messages affichés à l'écran

– elle affiche le bulletin de vote électronique

– elle accepte et valide le vote émis par l'électeur

– elle transcrit le vote sur la carte magnétique

– elle permet à l'électeur de revisualiser le vote qu'il a émis.

La disquette maîtresse contenue dans l'enveloppe scellée que le président peut ouvrir le jour des élections est une disquette d'initialisation (DOS amorçable) utilisée pour faire démarrer les machines à voter. C'est la même disquette qui a été utilisée au préalable pour activer l'urne-PC (voir plus loin). En effet, le logiciel détecte automatiquement s'il s'agit d'une machine à voter ou d'une urne-PC et de quel type (Digivote ou Jites).

Après son démarrage, la machine à voter affiche un pavé numérique à l'écran et invite le président à introduire son mot de passe. La machine à voter est alors opérationnelle.

Pour une machine à voter, un vote débute par l'insertion d'une carte magnétique validée. Le programme de vote contrôle si :

– la carte a été insérée correctement dans le lecteur, faute de quoi cette erreur est signalée à l'utilisateur;

– le contenu de la carte est lisible, sans quoi il est demandé à l'électeur d'en informer le président;

– la carte a été validée pour ce bureau de vote sans quoi il est demandé à l'électeur d'en informer le président.

Lorsque la carte a été insérée correctement, l'électeur peut émettre son vote au moyen d'un crayon optique. Pour sélectionner un élément, il y a lieu de poser le crayon optique perpendiculairement à l'écran sur la zone choisie et d'appuyer sur l'écran. En dehors de ces zones actives, le système ne tient pas compte des pressions sur le crayon.

Après le vote, la machine à voter enregistre sur la carte magnétique les données pour chaque élection pour laquelle l'électeur a émis un vote.

En outre, elle transcrit un bit de test qui indique que cette carte a effectivement servi à émettre un vote et un nombre de contrôle qui doit garantir l'intégrité du vote. Ce nombre de contrôle permettra à l'urne électronique de vérifier que le vote enregistré sur la carte magnétique est effectivement un vote correct émis avec une machine à voter du bureau de vote le jour des élections.

3.1.3.2 De urne-PC

De voorzitter zorgt met de urne-PC voor :

– het openen en sluiten van het stembureau;

– het initialiseren van de blanco magneetkaarten voor de kiezers;

– het aanvaarden van de magneetkaart met de uitgebrachte stem van de kiezer;

– het registreren van de uitgebrachte stem;

– het volgen van het verloop van de stemming;

– het op diskette schrijven van de resultaten van de stemming bij het afsluiten, deze zullen later dienen voor de totalisatie.

De urne-PC wordt opgestart met de master-diskette uit de verzegelde envelop. Tijdens de opstartfase wordt de apparatuur gecontroleerd op zijn goede werking. Na de opstartfase moet het paswoord worden ingegeven om de software te starten. Daarna wordt de master-diskette verwijderd uit de urne-PC en gebruikt als opstartdiskette voor de stemmachines met hetzelfde paswoord. Wanneer alle stemmachines zijn opgestart, in het geval van de Digivote-materiaal, wordt de master-diskette terug in de diskettelezer van de urne-PC geplaatst. Deze diskette zal voor de rest van de stemverrichtingen aanwezig blijven in de urne-PC en wordt gebruikt om de stemmen te registreren van de magneetkaarten die in de urne worden gedeponeerd.

Een belangrijk element in de veiligheid van het elektronisch stemmen is de initialisering van de magneetkaarten voor de kiezers met behulp van de urne-PC. Wanneer een kiezer zich aanbiedt dan neemt de voorzitter een magneetkaart en introduceert deze in de magneetkaartvalidatielezer van de urne-PC (niet te verwarren met de magneetkaartlezer in het deksel van de urne bevestigd aan de urne-PC). Bij deze operatie wordt een blanco stem op de magneetkaart voor de kiezer geschreven samen met een controlegetal. Het schrijven van de blanco stem tijdens de initialisering is noodzakelijk omdat de kiezer niet verplicht is om zijn magneetkaart in de stemmachine te steken. Hij kan immers onmiddellijk zijn magneetkaart deponeren in de urne. Een niet-geïnitialiseerde kaart zal zowel door de stemmachine als de urne worden geweigerd.

De hoofdfunctie van de urne-PC is uiteraard het aanvaarden van de magneetkaarten met de uitgebrachte stemmen. De kiezer steekt zijn kaart, na een visuele controle door de voorzitter, in de magneetkaartlezer in het deksel van de urne. De urne-PC leest de magneetkaart en gaat na of deze geldig is. Is dit niet het geval dan wordt de magneetkaart uitgeworpen. Deze verificatie steunt op het controlegetal dat steeds mee wordt weggeschreven zowel bij de initialisering als bij de stemming zelf. Het controlege-

3.1.3.2. L'urne-PC

Avec l'urne-PC, le président est chargé :

– d'ouvrir et de fermer le bureau de vote;

– d'initialiser les cartes magnétiques vierges pour les électeurs;

– d'accepter la carte magnétique avec le vote émis par l'électeur;

– d'enregistrer le vote émis;

– de suivre le déroulement du vote;

– à la clôture, d'écrire les résultats des votes sur les disquettes qui serviront à la totalisation.

La disquette maîtresse contenue dans l'enveloppe scellée sert à faire démarrer l'urne-PC. Pendant la phase de démarrage, le bon fonctionnement du système est contrôlé. Après la phase de démarrage, il faut introduire le mot de passe pour lancer le logiciel. Ensuite, la disquette maîtresse est retirée de l'urne-PC et est utilisée comme disquette d'amorçage pour les machines à voter avec le même mot de passe. Dans les cas du matériel Digivote, lorsque toutes les machines à voter ont démarré, la disquette maîtresse est remise dans le lecteur de disquettes de l'urne. Elle restera dans l'urne pendant toutes les opérations de vote et servira à enregistrer les votes contenus sur les cartes magnétiques déposées dans l'urne-PC.

L'initialisation des cartes magnétiques pour les électeurs au moyen de l'urne-PC constitue un élément important dans la sécurité du vote automatique. Lorsqu'un électeur se présente, le président prend une carte magnétique et l'introduit dans la valideuse de cartes magnétiques de l'urne-PC (à ne pas confondre avec le lecteur de cartes magnétiques du couvercle de l'urne fixé à l'urne-PC). Lors de cette opération s'inscrivent, sur la carte magnétique de l'électeur, un vote blanc ainsi que le nombre de contrôle. L'inscription du vote blanc pendant l'initialisation est nécessaire parce que l'électeur n'est pas tenu d'insérer sa carte magnétique dans la machine à voter. En effet, il peut déposer immédiatement sa carte magnétique dans l'urne. Une carte non initialisée sera refusée, tant par la machine à voter que par l'urne.

Bien entendu, la fonction principale de l'urne-PC est d'accepter les cartes magnétiques contenant les votes émis. L'électeur insère sa carte, après un contrôle visuel du président, dans le lecteur de cartes magnétiques du couvercle de l'urne-PC. L'urne lit la carte magnétique et vérifie si celle-ci est valable, sans quoi elle l'expulse. Cette vérification repose sur le nombre de contrôle qui est à chaque fois transcrit, tant lors de l'initialisation que lors du vote même. Le nombre de contrôle est calculé sur la base du contenu

tal wordt berekend op basis van de inhoud van de stem van de kiezer. Bij het lezen van de magneetkaart berekent de urne-PC opnieuw dit controlegetal. Verschilt dit berekende controlegetal, van het controlegetal op de magneetkaart dan wijst dit ofwel op het feit dat de stem is gewijzigd na de registratie van de stem door een stemmachine, ofwel dat het controlegetal met een andere encryptiesleutel werd berekend dan deze van het stembureau. In de praktijk wijst deze laatste hypothese meestal op het feit dat de magneetkaart niet werd geïnitialiseerd, afkomstig is uit een ander bureau of dat deze defect is.

Een geldige magneetkaart, met andere woorden een kaart waarvoor het controlegetal klopt, wordt als zodanig gedetecteerd. Na registratie van de stem valt zij in de opvangbak.

Elke stem wordt geregistreerd in een bestand op de diskette in de urne-PC. De plaats waar de stem in dit bestand terechtkomt, is willekeurig en dus niet afhankelijk van de volgorde waarin de kiezers stemmen. Zo kan het geheim van de stemming worden bewaard. Elke stem in dit bestand is bovendien versleuteld.

Geraakt de diskette tijdens de stemoperaties beschadigd dan kan de urne-PC nog steeds verder werken in zogenaamde « beperkte modus ». Het blijft dan mogelijk om verder kaarten te initialiseren en om kaarten te deponeren in de urne. De registratie wordt echter wel stopgezet. In dit geval is men verplicht om, na het sluiten van het stembureau, de magneetkaarten te herstellen in het hoofdbureau. Dit wordt gedaan door alle kaarten die zich in de elektronische urne bevinden opnieuw, één voor één, door een magneetkaartlezer te laten inlezen.

Tijdens de verkiezingen toont de urne-PC een teller op het scherm met het aantal in de elektronische urne gedeponeerde kaarten.

Bij het sluiten van het stembureau totaliseert de urne-PC al de stemmen voor elke lijst en voor elke kandidaat. Deze informatie wordt echter niet zichtbaar gemaakt maar is wel in geëncrypteerde vorm beschikbaar op de master en de back-up diskettes. Bij de volgende fase in het hoofdbureau, waar de totalisatie van verschillende stembureaus zal gebeuren, wordt immers uitgegaan van deze informatie.

De werking van de Jites urne en van de Digivote urne zijn identiek behalve wat betreft het recupereren van de gegevens bij een panne de dag van de verkiezingen.

3.2. Het totalisatiebureau

3.2.1. De procedure

Onmiddellijk na ontvangst van de diskettes van het stembureau leest de voorzitter van het hoofdbureau de mas-

du vote de l'électeur. Lors de la lecture de la carte magnétique, l'urne recalcule ce nombre de contrôle. Si ce nombre de contrôle recalculé diffère du nombre de contrôle sur la carte magnétique, cela indique soit que le vote a été modifié après l'enregistrement du vote par une machine à voter, soit que le nombre de contrôle a été calculé avec une autre clef de chiffrement que celle du bureau de vote. Dans la pratique, cette dernière hypothèse indique la plupart du temps que la carte magnétique n'a pas été validée, qu'elle vient d'un autre bureau ou qu'elle est défectueuse.

Une carte magnétique valable, c'est-à-dire une carte où les deux nombres de contrôle correspondent, est détectée comme telle. Après enregistrement du vote, elle tombe dans le bac de réception.

Chaque vote est enregistré dans un fichier sur la disquette contenue dans l'urne-PC pour les systèmes Digivote et sur l'EEPROM pour les systèmes Jites. L'endroit où aboutit le vote dans ce fichier est arbitraire. Dès lors, il ne dépend pas de l'ordre dans lequel les électeurs votent. On peur ainsi garantir le secret du vote. En outre, chaque vote dans ce fichier est crypté.

Si la disquette est endommagée pendant les opérations de vote, l'urne peut encore travailler en mode dit « dégradé ». Il reste alors possible de continuer à initialiser des cartes et à les déposer dans l'urne. Toutefois, il n'y a plus d'enregistrement. Dans ce cas, on est obligé, après la fermeture du bureau de vote, de recompter les cartes magnétiques dans le bureau principal de commune en faisant relire une à une, par un lecteur de cartes magnétiques, toutes les cartes qui se trouvent dans l'urne électronique.

Pendant les élections, l'urne-PC affiche un compteur à l'écran avec le nombre de cartes déposées dans l'urne électronique.

Lors de la fermeture du bureau de vote, l'urne-PC totalise déjà les votes pour chaque liste et pour chaque candidat. Ces informations ne sont cependant pas visibles; elles sont disponibles sous une forme codée sur la disquette maîtresse et sur les disquettes de sauvegarde. En effet, ces informations sont utilisées lors de la phase suivante au bureau principal où intervient la totalisation des différents bureaux de vote.

Le fonctionnement de l'urne Jites et de l'urne Digivote sont identiques sauf en ce qui concerne la récupération d'informations après une panne pendant la journée de l'élection.

3.2. Le bureau de totalisation

3.2.1. La procédure

Immédiatement après la réception des disquettes du bureau de vote, le président du bureau principal lit la dis-

ter diskette in op een totalisatiemachine. De voorzitter van het stembureau ontvangt een bewijs voor de afgifte van zijn diskettes. Indien het lezen van de master diskette onmogelijk blijkt, herbegint de voorzitter van het hoofdbureau de registratieverrichting met de back-up diskettes van hetzelfde stembureau. Indien dit eveneens onmogelijk blijkt, eist de voorzitter van het hoofdbureau de overeenkomstige elektronische urne op.

In geval van Digivote materiaal gaat hij over tot het herstellen van de magneetkaarten uit de urne. De herstelde stemmen worden geregistreerd op diskette. De urne wordt na de hertelling opnieuw verzegeld en terug naar de gemeente gestuurd. Vervolgens leest de voorzitter de nieuw aangemaakte diskette in op de totalisatiemachine.

In het geval van de Jites hardware, kan een nieuwe diskette met de resultaten bekomen worden door de resultaten op de EEPROM in de urne op te vragen. Indien de EEPROM defect is, wordt op een gelijkaardige methode als voor de Digivote systemen overgegaan.

Een gemeente beschikt over één zogenaamde « tussenliggende » totalisatiemachine per dertig stembureaus. De uitslag van ieder bureau wordt geregistreerd op één welbepaalde tussenliggende totalisatiemachine, nooit op meerdere tegelijkertijd om dubbeltellingen te vermijden. Eenmaal alle stembureaus geregistreerd zal de zogenaamde « bovenliggende » totalisatiemachine van de gemeente alle tussenliggende resultaten (per 30 stembureaus) totaliseren tot een globaal resultaat voor de gemeente. Zijn er minder dan 30 stembureaus in een gemeente dan is er slechts één totalisatiemachine en verdwijnt het onderscheid tussen het tussenliggend en bovenliggend totalisatieniveau.

De afkondiging door de voorzitter van het hoofdbureau van gedeeltelijke verkiezingsuitslagen, kan pas gebeuren na de registratie van ten minste 10 bureaus en nadien per 10 bijkomende stembureaus, dit met het oog op het bewaren van het geheim van de stemming. Na de registratie van alle stembureaus drukt het systeem het proces-verbaal en de stemopnemingstabellen af. Dit proces-verbaal in meervoud en de verschillende stemopnemingstabellen die zijn ondertekend door de voorzitter van het hoofdbureau, de leden van het bureau en de getuigen, worden in verzegelde omslagen gestopt.

Tot aan de validatie van de verkiezingen blijven de omslagen met magneetkaarten en de diskettes onder toezicht van de voorzitter van het hoofdbureau. Ook de urnen met magneetkaarten blijven tot dan verzegeld.

3.2.2. Het totalisatiesysteem : apparatuur

De hardware van een totalisatiemachine bestaat uit een standaard PC met uitneembare of vaste harde schijf (Zipschijf). Het opstarten moet gebeuren vanaf een diskette met

quette maîtresse pour les disquettes. S'il s'avère impossible de lire la disquette maîtresse, le président du bureau principal recommence l'opération de lecture avec les disquettes de sauvegarde du même bureau de vote. Si l'opération s'avère aussi impossible, le président du bureau principal requiert l'urne électronique correspondante.

Dans le cas du matériel Digivote, il procède au recomptage des cartes magnétiques contenues dans l'urne. Les votes recomptés sont enregistrés sur disquette. Après le recomptage, l'urne est rescellée et renvoyée à la commune. Ensuite, le président enregistre la disquette nouvellement fabriquée sur la machine de totalisation.

Dans le cas du matériel Jites, une nouvelle disquette de résultats peut être obtenue en récupérant les données dans l'EEPROM de l'urne. Si l'EEPROM s'avère défectueuse il est procédé comme dans le cas du matériel Digivote.

Une commune dispose d'une machine de totalisation « intermédiaire » par série de 30 bureaux de vote. Le résultat de chaque bureau est enregistré sur une machine de totalisation intermédiaire déterminée, jamais sur plusieurs simultanément afin d'éviter les doubles comptages. Une fois tous les bureaux de vote enregistrés, la machine de totalisation « faîtière » de la commune totalisera tous les résultats intermédiaires (par série de 30 bureaux de vote) afin d'obtenir le résultat global de la commune. S'il y a moins de 30 bureaux de vote dans une commune, il n'y a alors qu'une seule machine de totalisation et la distinction entre niveau de totalisation intermédiaire et faîtier disparaît.

Le président du bureau principal peut proclamer des résultats électoraux partiels après enregistrement d'au moins 10 bureaux et par la suite par série de 10 bureaux de vote supplémentaires, ceci pour garantir le secret du vote. Après enregistrement de tous les bureaux de vote, le système imprime le procès-verbal et les tableaux de recensement des votes. Ce procès-verbal en plusieurs exemplaires et les différents tableaux de recensement des votes, signés par le président du bureau principal, les membres du bureau et les témoins, sont mis dans des enveloppes scellées.

Jusqu'à la validation des élections, les enveloppes contenant les cartes magnétiques et les disquettes restent sous la surveillance du président du bureau principal. Les urnes contenant les cartes magnétiques restent aussi scellées jusqu'à la validation des élections.

3.2.2. Le système de totalisation : matériel

Le matériel d'une machine de totalisation se compose d'un PC standard avec disque dur (disque Zip) ou fixe. Le démarrage doit se faire à partir d'une disquette et d'un mot

het bijhorend paswoord dat specifiek is voor elke totalisatiemachine. De totalisatiesoftware en -gegevens bevinden zich op de harde schijf.

3.2.3. Het totalisatiesysteem : werking

In essentie doet een totalisatiesysteem niets meer dan de diskettes van de stembureaus één voor één inlezen en de stemmen tellen voor elke lijst en voor elke kandidaat. Een totalisatiesysteem bestaat uit een magnetische informatiedrager waarop de nodige programma's en gegevens staan teneinde de totalisatiefuncties voor de verkiezingen op de verschillende niveaus te kunnen uitvoeren. De gegevens staan op het systeem onder de vorm van een database. De in deze database opgeslagen informatie omvat :

– de lijst van de stembureaus die door dit totalisatiesysteem moeten worden getotaliseerd; het systeem loet immers kunnen controleren of er geen stembureaus worden vergeten of dubbel geteld;

– de encryptiesleutels van de diskettes van de in te lezen stembureaus; de informatie op de master en back-up diskettes van de stembureaus is immers geëncrypteerd. Om deze informatie te kunnen lezen moet het totalisatiesysteem beschikken over de encryptiesleutels van de stembureaus. De database met de encryptiesleutels is op haar beurt geëncrypteerd met het paswoord van het totalisatiesysteem.

Alle gegevens, inclusief de berekende totalen, worden beschermd met controlegetallen.

4. Controle

4.1. Controles uitgevoerd voor de verkiezingen

4.1.1. Ontvangst en beschrijving van de verkiezingssoftware

4.1.1.1. Ontvangst van de verkiezingssoftware

Op 13 september 2006 heeft het Bureau van Dijk, adviesorgaan erkend door het MBHG (Ministerie van het Brussels Hoofdstedelijk Gewest), haar rapport voorgesteld over de definitieve versie van de verkiezingsprogrammatuur ontwikkeld door het bedrijf Stésud voor de verkiezingen van 8 oktober 2006. Dit verslag werd in aanwezigheid van vertegenwoordigers van het MBHG, Stésud en leden van het college toegelicht.

Na de presentatie werd het referentiemateriaal in aanwezigheid van vertegenwoordigers van alle aanwezige instanties ondergebracht in de kluis van het MBHG in een Dexia agentschap :

de passe spécifique à chaque PC de totalisation. Le logiciel et les données de totalisation se trouvent sur le disque dur.

3.2.3. Le système de totalisation : fonctionnement

Par essence, le système de totalisation ne fait rien d'autre qu'enregistrer une à une les disquettes des bureaux de vote et compter les voix pour chaque liste et pour chaque candidat. Un système de totalisation se compose d'un support d'information magnétique sur lequel figurent les programmes et les données nécessaires pour pouvoir effectuer aux différents niveaux les fonctions de totalisation pour les élections. Les données figurent sur le système sous la forme d'une base de données. Les informations contenues dans cette base de données comprennent :

– la liste des bureaux de vote qui doivent être totalisés par ce système de totalisation; le système doit en effet pouvoir contrôler si aucun bureau de vote n'a été oublié ou compté deux fois;

– les clefs de chiffrement des disquettes des bureaux de vote à enregistrer; en effet, les informations sur les disquettes maîtresses et de sauvegarde sont codées. Pour pouvoir lire ces informations, le système de totalisation doit disposer des clefs de chiffrement des bureaux de vote. La base de données avec les clefs de chiffrement est codée à son tour avec le mot de passe du système de totalisation.

Toutes les données, y compris les totaux calculés, sont protégées par des nombres de contrôle.

4. Contrôle

4.1. Contrôles effectués avant le jour des élections

4.1.1. Réception et description des logiciels électoraux

4.1.1.1. Réception des logiciel électoraux

Le 13 septembre 2006, le Bureau van Dijk, organisme d'avis reconnu par la MRBC (Ministère de la Région de Bruxelles-Capitale), a présenté son rapport sur la version définitive des logiciels électoraux développés pour les élections du 8 octobre 2006 par la firme Stésud. Ce rapport a été commenté en présence de représentants du MRBC, de la firme Stésud, fournisseur des logiciels et de membres du collège.

Après la présentations, le matériel de référence a été déposé au coffre du MRBC à la banque Dexia en présence de représentants de tous les organismes présents :

– een kopie van de broncode van de programma's;

– een demonstratieversie van de diskettes gebruikt tijdens de verkiezingen en de voorbereiding ervan.

Een kopie van de referentiesoftware werd genomen voor analyse door het college.

Op 26 september 2006 kreeg het college van Steria (Digivote systeem), de leveranciers van de pc's in 15 van de 19 Brusselse gemeentes, de broncode en een uitvoerbare versie van de diagnosediskette.

4.1.1.2. Beschrijving van de verkiezingssoftware

Vergeleken met de vorige verkiezingen, is er nu slechts één leverancier van software voor de twee hardware platformen (Digivote en Jites). In de verschillende fasen van de procedure wordt verschillende programmatuur gebruikt. In de dagen voor de verkiezingen worden de diskettes voor de stem- en telbureaus met een « voorbereidingssoftware » aangemaakt, de stemcomputers en urnen met « diagnosesoftware » gecontroleerd en geïntialiseerd. De dag van de verkiezingen worden de stemmen uitgebracht met de « stemprogrammatuur » en verzameld op de voorzittersmachine via de « urnesoftware ». In de hoofdbureaus worden de stemmen dan geteld door de « totalisatiesoftware ».

4.1.2. Tussenkomst van Bureau van Dijk

Artikel 2, § 2, van de wet van 11 april 1994 op de organisatie van de geautomatiseerde stemopneming schrijft voor dat de systemen gebruikt voor de geautomatiseerde stemopneming alsmede de systemen gebruikt voor de telling en de totalisatie moeten worden goedgekeurd door de minister van Binnenlandse Zaken.

Overeenkomstig dit artikel lanceerde de FOD Binnenlandse Zaken op 25 september 2002 een oproep tot kandidaatstelling met het oog op het aanduiden van een keuringsorganisme. Dit keuringsorganisme had tot taak de minister van Binnenlandse Zaken te adviseren met het oog op de goedkeuring van de betreffende systemen.

De firma Bureau van Dijk, die werd weerhouden tijdens deze procedure werd aangeduid als adviesorgaan voor de gemeenteraadsverkiezingen van 2006 in Brussel.

Volgens de oproep tot kandidatuurstelling verschenen in het *Belgisch Staatsblad* van 8 oktober 2002 zijn de taken van het adviesorgaan de volgende :

– aantonen dat het stemsysteem, zowel op het vlak van de hardware als de software, degelijk functioneert;

– une copie des sources des programmes;

– une version de démonstration des disquettes utilisées pour les élections et leur préparation.

Une copie des logiciels de référence a été reprise pour analyse par le collège.

Le 26 septembre 2006, le collège a reçu les sources et une version exécutable de la disquette de diagnostic des mains de la firme Stéria, fournisseur des machines de type Digivote, système utilisé dans 15 des 19 communes de la Région bruxelloise.

4.1.1.2. Description des logiciels électoraux

Contrairement aux élections précédentes, il n'y a qu'un seul fournisseur pour les logiciels de vote et de totalisation pour les deux plate-formes matérielles (Digivote et Jites). Selon les phases de la procédure, différents logiciels sont utilisés. Dans la période qui précède les élections, les disquettes pour les bureaux de vote et de totalisation sont préparées avec le « logiciel de préparation » et les machines à voter et les urnes sont contrôlées et initialisées à l'aide d'un « logiciel de diagnostic »; le jour des élections, les votes sont émis grâce au « logiciel de vote » et rassemblés dans l'urne à l'aide du « logiciel urne ». Dans les bureaux principaux, les votes sont totalisés à l'aide du « logiciel de totalisation ».

4.1.2. 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 doit être agréé par le ministre de l'Intérieur.

Conformément à cet article, le 25 septembre 2002, le SPF Intérieur lançait un appel à candidatures en vue de désigner les organismes chargés de remettre un avis au ministre de l'Intérieur sur les fournisseurs de ces systèmes.

La société Bureau van Dijk, retenue lors de cette procédure, a été désignée comme organisme d'avis pour les élections communales de 2006 à Bruxelles.

Selon l'appel à candidatures paru au *Moniteur belge* du 8 octobre 2002, les tâches de l'organisme d'avis sont de :

– vérifier que le système fonctionne correctement, tant au niveau des composantes matérielles que logicielles;

– aantonen dat het stemsysteem de actuele kieswetgeving, alsmede de taalwetgeving volledig en correct respecteert;

– aantonen dat het stemsysteem rekening houdt met de wettelijk beschikbare tijd voor het aanmaken van de stemdiskettes voor de stembureaus en de kantonhoofdbureaus;

– aantonen dat het stemsysteem niet tijdrovend is bij de inwerkingstelling van het stemsysteem door het stembureau en voor de kantonhoofdbureaus;

– aantonen dat het stemsysteem gebruiksvriendelijk is voor de kiezers;

– aantonen dat een volledige documentatie en een bruikbare handleiding door de leveranciers worden geleverd;

– de ontvangst en de controle van de basissoftware met de broncodes, de bewaring van de software, de voorbereiding van de stemming en de controle van het stemmateriaal (hardware en software) in het stembureau en voor de totalisatie van de stemming in het kantonhoofdbureau nagaan;

– de werking van het stemmateriaal in de opeenvolgende stappen van de verkiezingsketen nagaan;

– de werking en de oplossing bij verkeerde manipulaties van het stemmateriaal bij de aanmaak van de stemdiskettes, de stemming en de totalisatie van de stemmen, alsook bij stroomuitval van het stemsysteem in een stembureau nagaan.

Artikel 2, § 2, van de wet van 11 april 1994 bepaalt dat een stemsysteem de betrouwbaarheid en de veiligheid van de systemen, alsmede het geheim van de stemming moet garanderen.

Op basis van de adviezen uitgebracht door Bureau van Dijk heeft de MBHG het stem- en stemopnemingssysteem goedgekeurd.

Het college was aanwezig bij de overhandiging van deze verslagen aan de MBHG, in aanwezigheid van de vertegenwoordigers van Bureau van Dijk en van de leverancier. Het college heeft een kopie ontvangen van dit advies.

Het college is van mening dat de gevolgde procedure van goedkeuring de betrouwbaarheid van de stemsystemen en van de stemopnemingssystemen verhoogd.

De commerciële band die de softwareleverancier en het adviesorgaan bindt, is het niet van dien aard dat ze de noodzakelijke onafhankelijkheid van dat adviesorgaan garandeert. Het college meent dat die commerciële band niet kan worden afgeleid uit de wet of de oproep tot kandidatuurstelling voor het adviesorgaan. Het college beveelt daarom aan, dat dit wordt herzien.

– vérifier que le système est rigoureusement conforme à la législation électorale et linguistique actuelle;

– vérifier que le système tient compte du délai prévu par la loi pour la confection des disquettes de vote destinées aux bureaux de vote et aux bureaux principaux de canton;

– vérifier que le système ne prend pas trop de temps au démarrage dans les bureaux de vote et dans le bureaux principaux de canton;

– vérifier que le système est convivial pour les électeurs;

– vérifier que le système est accompagné d'une documentation complète et d'un manuel d'utilisation pratique;

– tester la réception et le contrôle du logiciel de base avec les codes sources, la conservation du logiciel, la préparation du scrutin, le contrôle du système de vote (hardware et software) dans le bureau de vote et dans le bureau principal de canton pour la totalisation des votes;

– tester le fonctionnement du système de vote au long des étapes successives de la chaîne électorale;

– tester le fonctionnement et la solution envisagée en cas d'erreur de manipulation du matériel de vote lors de la confection des disquettes de vote, lors du vote et lors de la totalisation des voix, ainsi qu'en cas de panne de courant survenant dans un bureau de vote.

L'article 2, § 2, de la loi du 11 avril 1994 précise qu'un système de vote doit garantir en tout cas la fiabilité et la sécurité des systèmes, ainsi que le secret du vote.

Le MRBC a agréé le système de vote et de dépouillement électronique sur la base de l'avis émis par le Bureau van Dijk.

Le collège a assisté à la remise de ces avis au MRBC en présence des délégués du Bureau van Dijk et du fournisseur. Le collège a reçu une copie de cet avis.

Le collège estime que cette procédure d'agrément ne peut qu'augmenter la fiabilité des systèmes de vote et de dépouillement.

Le lien commercial qui lie le fournisseur de logiciel et l'organisme d'avis lors de la mission de celui-ci n'est pas de nature à garantir le caractère d'indépendance indispensable à cette mission. Le collège est par ailleurs d'avis que ce lien commercial ne peut être déduit ni de la loi, ni de l'appel à candidatures pour l'organisme d'avis. Il recommande dès lors qu'il soit revu.

Talrijke functionele test werd uitgevoerd met de programmatuur op het materiaal. Het college stelt wel vast dat het adviesorgaan de broncode van de verkiezingssoftware slechts gedeeltelijk heeft geanalyseerd.

De overheden belast met de organisatie van de verkiezingen zouden de kwaliteit en de doeltreffendheid van de broncode in een audit moeten laten onderzoeken. Daarom zou de software enkele maanden voor de dag van de verkiezingen klaar moeten zijn.

De autoriteiten zouden eveneens alle procedures bij het voorbereiden van de verkiezingen, de verkiezingen zelf en de totalisatie in een audit moeten laten evalueren.

4.1.3. Analyse van de inhoud van de diskettes

Deze analyse gaat na of de programma's op de diskettes gebruikt de dag van de verkiezingen, dezelfde zijn als deze overhandigd aan het college.

Daarvoor voert het college een onafhankelijke referentiecompilatie uit.

De dag van de verkiezingen hebben de deskundigen kopieën genomen van de diskettes gebruikt in de stembureaus. De avond van de verkiezingen werden ook in sommige totalisatiebureaus kopieën genomen van de diskettes uit de stembureaus die werden gebruikt voor de totalisatie. In de dagen na de verkiezingen hebben de deskundigen de resterende diskettes, gebruikt bij de totalisatie, gekopieerd.

De uitvoeringscode bekomen uit de referentiecompilatie werd vergeleken met de programmatuur verzameld door het college en toonde geen verschil.

4.1.3.1. Referentieomgeving

Een pc van het college werd gebruikt om zowel de diagnose- als de stemprogrammatuur te hercompileren. Op die « maagdelijke » pc (gecontroleerd op virussen en niet in een netwerk opgenomen) werd de Borland C++ (versie 3.1 voor DOS) ontwikkelomgeving met de originele diskettes geïnstalleerd.

4.1.3.2. Diagnosediskette

De diagnosediskette voor de Digivote hardware bevat software ontwikkeld door de hardwareleverancier Digivote om de pc's uit de stembureaus te controleren op mogelijke hardware fouten en de machines klaar te maken voor het gebruik de dag van de verkiezingen. Mogelijke randapparatuur onnodig voor de verkiezingen (harde schijf, Cd-romle-

Si de nombreux tests fonctionnels ont été réalisés sur le matériel et les logiciels des élections, le collège constate que seule une analyse partielle du code des logiciels des élections a été réalisée.

Les autorités en charge des élections devraient faire procéder à un audit sur la qualité et la pertinence du code source des logiciels des élections. Pour ce faire, le code définitif des logiciels devrait être finalisé plusieurs mois avant le jour des élections.

Les autorités devraient également faire procéder à un audit de toutes les procédures intervenant dans la préparation des élections et de opérations de vote et de totalisation.

4.1.3. Analyse du contenu des disquettes

L'objectif de cette analyse est de vérifier que les programmes présents sur les disquettes utilisées pour les élections et leur préparation correspondent exactement aux sources remises au collège.

Le collège a, à cette fin, effectué une compilation de référence indépendante.

Le jour des élections, les experts ont pris des copies des disquettes utilisées dans les bureaux de vote. Le soir des élections, dans certains bureaux de totalisation, ils ont également pris des copies des disquettes provenant des bureaux de vote et utilisées pour la totalisation. Enfin, dans les jours qui ont suivi les élections, les experts ont également pris des copies des disquettes utilisées pour la totalisation dans toutes les communes.

Les exécutables de la compilation de référence ont été comparés avec les copies récoltées et se sont révélés identiques.

4.1.3.1. Environnement de référence

Un PC a été préparé par le collège pour la recompilation du logiciel de diagnostic et des logiciels de vote. La version d'origine du compilateur Borland C++ 3.1 pour DOS a été installée sur ce PC « vierge », contrôlé contre les virus et placé en dehors d'un réseau.

4.1.3.2. Disquette de diagnostic

La disquette de diagnostic pour le matériel de type Digivote contient un logiciel développé par le fournisseur des systèmes Digivote qui identifie les éventuelles pannes hardware et prépare les machines pour le jour des élections. Les périphériques inutiles pour les élections sont désactivés (disques durs, CD-rom, …) par le programme. En plus

zer, …) wordt buiten gebruik gesteld. Naast de programmatuur van de leverancier (Steria) is er ook software geleverd door de constructeur van de hardware : stuurprogramma's voor de lichtpen, kaartlezers, programmatuur om informatie te lezen en te schrijven in de BIOS van de pc's en het besturingssysteem. Het college beschikte enkel over de broncode van de programmatuur van de hardwareleverancier (Steria).

Na hercompilatie en comprimeren van de uitvoeringscode bleken die binair identiek met de programmatuur verkregen door het college.

4.1.3.3. Diskette voor de stembureaus

De programmatuur in de stembureaus is identiek, onafhankelijk van het type hardware (Jites, Digivote) en functie (stemcomputer of urne), voor elk bureau. Bij het opstarten van de machine wordt het type en de functie van de pc automatisch bepaald en, wordt ofwel de stemsoftware, ofwel de urne opgestart.

Van vier op de vijf uitvoerbare programma's (.exe) aanwezig op de diskette beschikte het college over de broncode. Na hercompilatie van die broncode bleek de uitvoeringscode binair identiek met de vooraf door de softwareleverancier overhandigde programmatuur.

Naast de programmatuur van de leverancier is er ook software geleverd door de constructeur van de hardware : stuurprogramma's voor de lichtpen (onder andere het vijfde uitvoerbare programma), kaartlezers en het besturingssysteem (Microsoft DOS 6.20).

de ce logiciel, la disquette contient le système d'exploitation et des drivers spécifiques développés par les fabricants des périphériques : crayon optique, lecteurs de carte, lecture/écriture dans le BIOS. Le collège ne dispose que des sources développées par le fournisseur de hardware (Stéria).

Après recompilation et compression des exécutables, la comparaison binaire indique que les exécutables présents sur la disquette de diagnostic sont identiques à ceux obtenus par le collège.

4.1.3.3. Disquette pour les bureaux de vote

Le logiciel des bureaux de vote est identique pour tous les bureaux de vote. Ce logiciel est indépendant du type de matériel (Jites ou Digivote) et de la fonction du PC (machine à voter ou urne). Au démarrage de la machine, le type de matériel et la fonction du PC sont déterminés automatiquement et, soit le logiciel de vote, soit celui de l'urne, est démarré.

Le collège dispose des sources de quatre des cinq exécutables présents sur la disquette. Après recompilation du code source dans l'environnement de référence, il apparaît que les programmes exécutables obtenus sont identiques à ceux livrés par le fournisseur.

La disquette des bureaux de vote contient, en plus des programmes développés par le fournisseur, le driver du crayon optique (le cinquième programme) et le système d'exploitation (Microsoft DOS 6.20).

Inhoud van de diskettes voor de stembureaus

Contenu des disquettes pour les bureaux de vote

DOS 6.20 systeembestanden Fichiers système DOS 6.20	CONFIG.SYS, HIMEM.SYS, INIT.EXE, I.SYS, KEYB.COM, KEYBOARD.SYS, MSDOS.SYS, RAMDRIVE.SYS, COMMAND.COM
Lichtpen stuurprogramma's Drivers du crayon optique	DZINE.COM, LPCAL.DAT, PXL_BIOS.COM, PXLBIOS1.DTA, PXLBIOS2.DTA, TEST.EXE
Parameterbestanden, specifiek voor elk stembureau Fichiers de paramètres, spécifiques à chaque bureau de vote	BE.2, FLOPPY.BE, MACHVOTC.TBL, MACHVOTL.TBL, MACHVOTS.IND, MACHVOTS.TBL, URNE.IND, URNE.TBL, X.DSK
Stemprogramma en urneprogramma Programme de vote et programme urne	AUTOEXEC.BAT, BLANC.EXE, DRV.EXE, HARDDETC.EXE, MAV.BAT, MAVDIGIT.BAT, MAVJITES.BAT, RUNMAV.BAT, RUNURN.BAT, URNE.EXE

4.1.4. Analyse van de procedures

Het college heeft verschillende veiligheidsaspecten van de procedures voor de elektronische kiesverrichtingen onderzocht. Hoewel tijdens de evaluatie geen ernstig risico

4.1.4. Analyse des procédures

Le collège a examiné différents aspects liés à la sécurité des procédures du vote automatisé. Si aucun risque majeur n'a été identifié au cours de ces vérifications, le collège a

werd vastgesteld, heeft het college toch ondermeer de hierna volgende potentiële risico's overwogen :

– In zijn huidige versie kan, omwille van veiligheidsredenen, de broncode van de software van de kiesverrichtingen niet openbaar gemaakt worden voor de dag van de verkiezingen. Nochtans is de publicatie ervan vroeger dan de dag van de verkiezingen een wijze om het zekerheidsgevoel van de kiezers te versterken en hun vertrouwen in de elektronische kiesverrichtingen te verbeteren. Het publiek maken van de broncode van de software van de kiesverrichtingen veronderstelt de weglating eruit van de vier lettertekens die eigen zijn aan de huidige verkiezing en die daarin aanwezig zijn.

– De vier lettertekens die op unieke wijze verbonden zijn aan de huidige verkiezingen mogen op geen enkele evidente wijze deel uitmaken van de broncode van de software van de kiesverrichtingen. Deze broncode dient publiek gemaakt te worden voor de dag van de verkiezingen.

– Het is nodig om zich ervan te verzekeren dat de disketten gebruikt om de verschillende machines van een kiesbureau op te starten, niet besmet zijn door een softwarevirus (of andere destructieve software). Een procedure garandeert de niet-infectie van de diskettes en de software. Men moet zich er ook van vergewissen dat de diskettes niet geïnfecteerd zijn tussen het ogenblik van het openen van de verzegelde omslag waarin de diskettes geleverd worden, en het ogenblik dat ze gebruikt worden om de machines van een kiesbureau op te starten.

– Een veiligheidspolitiek dient opgesteld te worden om ondermeer maatregelen te nemen ten einde de software en digitale opslagmiddelen te beschermen tegen programmatuur van slechte wil. Een dergelijke veiligheidspolitiek moet ook de regels omvatten voor het ontwerpen van software, het versturen van zowel software als gegevens, de vertaling van de broncode naar machinecode, de aanmaak van de diskettes en het versturen ervan.

– Het verpakken van de diskettes in een omslag (ter bestemming van de voorzitters van de kiesbureaus) dient gepaard te gaan met een verzegeling van deze omslagen op een gewaarborgd veilige manier (een gebroken zegel mag niet op eenvoudige wijze kunnen worden hersteld, vervangen of vervalst). De procedures moeten voorzien dat de leden van een kiesbureau controleren en getuigen dat de omslag die de diskettes bevat en die aan de voorzitter van het kiesbureau overhandigd werd, wel degelijk verzegeld was op het ogenblik van de opening van het kiesbureau.

– Het moet verboden zijn om een computer binnen te brengen in het kiesbureau, met uitzondering van de computers eigen aan het kiesbureau (en van de machi-

entre autres considéré les diverses situations potentiellement à risque suivantes :

– Dans sa version actuelle, pour des raisons de sécurité, les sources des logiciels des élections ne peuvent être rendues publiques avant le jour des élections. Néanmoins, la publication de ces sources avant le jour des élections est une manière de renforcer le sentiment de confiance que peuvent ressentir les électeurs en regard du système de vote automatisé. La publication des sources des logiciels nécessite d'en soustraire les quatre caractères propres à l'élection en cours qui y apparaissent.

– Les quatre caractères associés univoquement à une élection ne devraient pas faire partie tels quels des sources des logiciels des élections. Les sources des logiciels des élections devraient être publiées avant le jour des élections.

– Il est nécessaire de s'assurer que les disquettes utilisées pour démarrer les différentes machines d'un bureau de vote ne sont pas contaminées par des virus informatiques (et autres logiciels malveillants). Une procédure garantit la non-infection des disquettes et des logiciels. Il faudrait aussi s'assurer que ces disquettes ne sont pas infectées entre le moment de l'ouverture des enveloppes qui les contiennent et le moment où les disquettes sont utilisées pour la totalisation.

– Une politique de sécurité décrivant, entre autres, l'ensemble des mesures mises en place pour protéger les logiciels et les supports utilisés contre les programmes malveillants devrait être rédigée. Une telle politique de sécurité détaillerait aussi les règles imposées quant à la conception des logiciels, la transmission des logiciels, la transmission des données, la compilation des logiciels, la création des disquettes et la transmission de ces disquettes.

– Lors de la mise sous enveloppe des disquettes (à destination finale des présidents de bureaux de vote), ces enveloppes devraient être scellées d'une manière sécurisée (un sceau brisé ne pouvant être reconstitué, remplacé ou falsifié aisément). Les procédures devraient prévoir que tous les membres d'un bureau de vote vérifient et attestent, au moyen d'un document à signer, que l'enveloppe contenant les disquettes reçue par le président du bureau est bien toujours scellée à la constitution du bureau de vote.

– En dehors des ordinateurs nécessaires aux procédures de votes, l'introduction dans un bureau de vote d'un ordinateur tiers devrait être interdite (à l'exception des ordi-

nes die nodig zouden zijn voor de helpdesktechnici en voor de deskundigen belast met de controle van de geautomatiseerde stemming).

– Rekening houdende met de leeftijd van het gebruikte materiaal, zou het de bescherming van de BIOS-parameters van de verschillende machines via een paswoord kunnen omzeild worden. Op deze wijze zou randapparatuur kunnen toegevoegd of uitgeschakeld worden.

– De diskettelezers, alsook de contacten aan de achterzijde van de verschillende machines, mogen niet toegankelijk zijn voor de kiezers.

– In een volgende versie van de geautomatiseerde stemming zou het wenselijk zijn de kiezer de zekerheid te geven over de overeenkomst tussen de uitgebrachte stem en de inhoud van de magneetkaart. De gebruikte drager (magneetkaart of andere) voor de geautomatiseerde stemming zou moeten toelaten de stem zowel elektronisch als rechtstreeks leesbaar voor de kiezer op te nemen (bijvoorbeeld afgedrukt in tekstvorm op de kaart).

4.1.5. Analyse van de broncode

Hoewel de beschikbaarheid van de broncode in principe de mogelijkheid biedt de werking van het systeem grondig te testen, is een volledige herlezing van de broncode niet kunnen gebeuren binnen de mogelijkheid aan tijd en middelen, toegemeten aan het college. Het college hechtte vooral belang aan de analyse van de meest kritieke punt in de programmatuur.

4.1.5.1. Gebruikte programmeertalen en ontwikkelomgevingen

De « voorbereidingssoftware » werd ontwikkeld in GUPTA (een 4GL ontwikkeltool). De « diagnosesoftware » in C++ en Assembler. De programma's voor de stemmachines en urne-pc's werden geschreven in C++ en C (routines voor encryptie en decryptie) en werden volledig binnen de Borland C/C++ ontwikkelingsomgeving (versie 3.1 voor DOS) gecompileerd. De programma's voor de totalisatie werden geschreven in Clipper.

4.1.5.2. De diagnosesoftware

Twee maal voor de verkiezingen wordt op de stem- en voorzittersmachines een diagnoseprogramma uitgevoerd. Dit programma controleert de goede werking van alle componenten van de machines en, in het geval van de systemen Digivote, schakelt de tijdens de verkiezingen onnodige randapparatuur uit.

Men mag niet vergeten dat dit soort test feilbaar is : men kan alleen de inzetbaarheid van de machine vast stellen

nateurs qui seraient nécessaires aux techniciens du helpdesk ou de ceux des experts chargés du contrôle du vote automatisé).

– Etant donné l'âge du matériel utilisé, la protection des paramètres des BIOS des différentes machines par un mot de passe pourrait être contournée. Des périphériques pourraient ainsi être rajoutés ou désactivés.

- Tout comme les lecteurs de disquettes, les connecteurs, qui se trouvent à l'arrière des différentes machines, devraient être rendus physiquement inaccessibles.

- Dans une prochaine mouture du vote automatisé, il serait souhaitable de donner plus de garantie à l'électeur quant à la correspondance entre le vote qu'il a émis et le contenu de la carte magnétique. Le support utilisé (carte magnétique ou autre) pour le vote automatisé devrait donc permettre d'enregistrer le vote tant de manière informatique que directement visible pour l'électeur (par exemple impression sous forme de texte sur la carte).

4.1.5. Analyse du code source

Bien que la disponibilité du code source permette d'analyser le logiciel de façon approfondie, le court délai et les moyens du collège n'ont pas permis une relecture intégrale du code source. Le collège s'est attaché à analyser les parties les plus critiques du logiciel.

4.1.5.1. Langages et outils de développement utilisés

Le « Logiciel de préparation » a été développé en GUPTA (outil de développement 4GL). Le « logiciel de diagnostic » a été écrit en C++ et en Assembler. Les programmes pour les machines à voter et les urnes ont été écrits en C++ et C (routines d'encryptage/décryptage) et ont été compilés dans l'environnement de développement Borland C/C++ (version 3.1. pour DOS). Les programmes pour la totalisation ont été rédigés en Clipper.

4.1.5.2. Logiciel de diagnostic

A deux reprises avant les élections, un programme de diagnostic est exécuté sur les machines à voter et les machines des présidents (urnes). Ce programme vérifie le bon fonctionnement de tous les composants des machines et, dans le cas des systèmes Digivote, désactive les périphériques inutiles pour l'élection.

Il faut noter que ce type de test n'est pas dans faille : il permet seulement de constater l'opérationnalité des machi-

zonder garantie dat dit de dag van de verkiezingen nog zo zal zijn. Hoewel sommige machines met succes werden getest de dag voor de verkiezingen, konden sommige stembureaus niet opstarten de dag zelf.

4.1.5.2.1. Diagnose van de Digivote-apparatuur

De broncode van de diagnosesoftware (versie 6.1) voor Digivotesystemen werd op 26 september door de constructeur aan het college voorgesteld.

Een vlugge analyse van die broncode leert dat het programma de volgende verrichtingen uitvoert :

– De generatie van het materiaal wordt bepaald : Digivote I, II, Iib of Iic

– Het serienummer van de machine wordt bepaald

– De bios-gegevens van de machine worden op diskette weggeschreven

– De goede werking van alle componenten van de stemmachines en de voorzittersmachines met inbegrip van de urne en de lichtpen wordt gecontroleerd. Er wordt een intensieve controle op de magnetische kaartlezers verricht. Het kalibreren van de lichtpen wordt eveneens op dit ogenblik uitgevoerd

– Onnodige randapparatuur wordt uitgeschakeld

– De testresultaten worden op diskette bewaard

– De testresultaten worden op het scherm getoond

Op de dag van de verkiezingen kan het programma in « wizardmode » worden gebruikt om mogelijke defecten op te sporen.

4.1.5.2.2. Diagnose van de Jitesapparatuur

Er is geen specifiek controleprogramma voor de Jitesmachines. Deze machines zijn speciaal gebouwd voor verkiezingsverrichtingen en kunnen niet worden aangepast. De apparatuur wordt getest met een demonstratieprogramma. Dit programma is identiek aan de software gebruikt op de dag van de verkiezingen maar gebruikt fictieve kieslijsten. De analyse van dit programma bevindt zich verder in de tekst.

4.1.5.3. Voorbereidingssoftware

Het college heeft de voorbereidingssoftware niet geanalyseerd. Dat programma maakt de diskettes en de overeenkomstige paswoorden voor elk stem- en telbureau aan. Alleen het resultaat van deze voorbereiding werd door het college bestudeerd.

nes au moment du test, sans autre garantie pour le jour des élections. Ainsi, quelques bureaux de vote n'ont pu démarrer bien qu'ayant été testés avec succès la veille.

4.1.5.2.1. Diagnostic pour les systèmes Digivote

Le code source du logiciel de diagnostic de Digivote (version 6.1) a été présenté au collège par le constructeur le 26 septembre 2006.

Une rapide analyse du code source indique que le programme effectue les opérations suivantes :

– La détection de la génération du matériel : Digivote I, II, IIb ou Iic.

– La détection du numéro de série de la machine.

– Le sauvetage des données du bios de la machine sur la disquette.

– Le contrôle du bon fonctionnement de tous les composants des machines à voter et des machines des présidents de bureau de vote, y compris l'urne et le crayon optique. Un contrôle intensif est effectué sur les lecteurs de cartes magnétiques. Le calibrage du crayon optique est également effectué à ce moment.

– La désactivation des composants inutiles.

– Le sauvetage sur la disquette du résultat des tests.

– L'affichage des résultats à l'écran.

Utilisé avec certains paramètres, le programme peut être exécuté en mode « wizard » pour tenter d'identifier d'éventuelles pannes le jour de l'élection.

4.1.5.2.2. Diagnostic pour le système Jites

Le système Jites n'a pas de logiciel spécifique pour les diagnostics. S'agissant de machines construites pour les opérations électorales exclusivement et ne pouvant donc être modifiées, les test effectués le sont à partir d'un programme de démonstration, identique à celui qui tourne le jour de l'élection mais avec des listes fictives. L'analyse de ce programme se trouve plus bas dans le texte.

4.1.5.3. Logiciel de préparation

Le logiciel de préparation n'a pas été analysé par le collège. La fonction de ce logiciel est de créer les disquettes et les mots de passe correspondants pour chaque bureau de vote et de totalisation. Seul le résultat de cette préparation a été étudié par le collège.

4.1.5.4. Stemsoftware

Naar gelang de gemeente worden twee soorten materiaal gebruikt : het Jitessysteem (4 gemeentes) en het Digivotesysteem (15 gemeentes). In beide gevallen worden de uitgebrachte stemmen bewaard in RAM geheugen (vluchtig) en op een niet-vluchtige drager. Bij Jites gaat het hier om een EEPROM en bij Digivote om de programmadiskette.

De drie stembureaudiskettes (1 master en 2 backups) worden in een verzegelde enveloppe bewaard, het paswoord van de voorzitter in een tweede verzegelde enveloppe. Enkele dagen voor de verkiezing krijgen de voorzitters deze twee enveloppen.

De programmadiskettes worden met het stembureaupaswoord (éénduidig en eigen aan het stembureau) gehandtekend. De pc van de voorzitter en de stemmachines kunnen alleen met dit paswoord worden opgestart.

Om de veiligheid te versterken zou het opportuun zijn om het wachtwoord van de diskettes te scheiden tot het moment van de start van de stemlokalen.

4.1.5.4.1. Opstarten van de machine van de voorzitter

Na het opstarten van de pc, controleert het programma aan de hand van de bestanden op de diskette en/of de inhoud van de EEPROM of de urne al werd gebruikt. Als de urne nog niet eerder werd gebruikt, start het systeem normaal op. Als de urne al was afgesloten, wordt dit aangegeven en start de urne niet op. Werd de urne al eerder gebruikt maar is ze nog niet afgesloten (bijvoorbeeld bij een stroompanne) en bevinden er zich al stemmen in de urne, dan gaat het systeem na of de urne hoort bij het stembureau en bij de lopende verkiezing. Indien dit het geval is, vraagt het systeem of de al ingelezen stemmen (in de urne) moeten worden bewaard of het systeem moet worden herinitialiseerd. In het eerste geval worden de stemmen aanwezig op de diskette of in EEPROM opnieuw in RAM geplaatst. In het tweede geval worden de RAM en de diskette (Digivote) of de EEPROM (Jites) bestanden geïnitialiseerd.

De stemverrichtingen kunnen beginnen : de magneetkaarten kunnen worden gevalideerd en de urne kan de uitgebrachte stemmen ontvangen.

4.1.5.4.2. Initialisatie van de stemkaarten

Het nalezen van de broncode laat ons vaststellen :

De stemkaarten moeten worden geïnitialiseerd voordat ze kunnen worden gebruikt in de stemmachines. Een jeton eigen aan het stembureau wordt door de valideringsma-

4.1.5.4. Logiciel de vote

Deux types de matériel différents sont utilisés selon les communes : le système Jites (4 communes) et le système Digivote (15 communes). Dans les deux cas, les votes émis sont conservés en mémoire RAM (volatile) et sur un support non volatile. Dans le cas de Jites, il s'agit d'une EEPROM, dans celui de Digivote, de la disquette de programme.

Les trois disquettes du bureau de vote (1 master - disquette maîtresse -, 2 backups) sont placées dans une enveloppe scellée. Le mot de passe du bureau de vote est placé dans une autre enveloppe scellée. Les deux enveloppes sont remises au président dans les jours qui précèdent l'élection.

La disquette des programmes est signée à l'aide d'un mot de passe unique et spécifique au bureau de vote. La machine du président et les machines à voter ne peuvent être démarrées qu'avec ce mot de passe.

Pour renforcer la sécurité, il serait opportun de séparer le mot de passe des disquettes jusqu'au moment du démarrage des bureaux de vote.

4.1.5.4.1. Démarrage de la machine du président

Après démarrage du PC, le programme vérifie, à partir du contenu des fichiers de la disquette et/ou de l'EEPROM, que l'urne n'a pas encore été utilisée. Si l'urne n'a pas encore été utilisée, le système démarre normalement. Si l'urne est clôturée, le système le signale et ne démarre pas. Si l'urne a été utilisée mais n'a pas encore été clôturée (cas de coupure de courant par exemple) et que des votes se trouvent déjà dans le fichier urne, le système vérifie que l'urne correspond bien au bureau de vote et à l'élection en cours. Si c'est le cas, le système demande s'il faut conserver les votes enregistrés (dans l'urne) ou s'il faut la réinitialiser. Dans le premier cas, les fichiers présents sur disquette ou dans l'EEPROM sont récupérés et replacés en RAM. Dans le second, les fichiers urne en RAM et sur la disquette (Digivote) ou sur l'EEPROM (Jites) sont initialisés.

Les opérations de vote peuvent commencer : la valideuse de carte est prête pour initialiser les cartes et l'urne est prête à recevoir les votes émis.

4.1.5.4.2. Initialisation des cartes à voter

La lecture des codes sources permet de constater les éléments suivants :

Les cartes à voter doivent être initialisées pour être utilisables dans les machines à voter. Un jeton spécifique au bureau de vote est écrit sur la carte introduite dans la vali-

chine op de kaart geschreven. Als de kaart al is beschreven, wordt ze door de valideringsmachine geweigerd en hoort men een geluidssignaal (behalve als de gegevens afkomstig zijn van vorige verkiezingen, dan wordt ze geïnitialiseerd).

4.1.5.4.3. Stemmachinesoftware

Het nalezen van de broncode laat ons het volgende vaststellen:

– De stemmachine kan alleen worden opgestart met het paswoord van de voorzitter van het stembureau.

– Alleen de magneetkaarten geïnitialiseerd op de pc van de voorzitter kunnen worden gebruikt in de stemmachines.

– De kiezer kan na het uitbrengen van zijn stem, het resultaat nakijken door de magneetkaart in eender welke stemmachine in te brengen. Hij kan zijn stem niet meer wijzigen. Deze controle laat geen spoor na de magneetkaart. Het nakijken van de stem kan dus zo veel maal herhaald worden als gewenst.

– De stemmen uit het geheugen van de stemmachine worden gewist (op nul gezet) na het uitwerpen van de magneetkaart. Voordat de uitgeworpen kaart in de urne wordt ingelezen is het alleen die magneetkaart die de uitgebrachte stem bevat.

– Naast de uitgebrachte stem bevat de magneetkaart een CRC die toelaat dat de urne de geldigheid van de magnetisch spoor controleert. Deze stem wordt, wegens plaatsgebrek op de kaart niet versleuteld.

4.1.5.4.4. Invoeren van een stemkaart in de urne

Wanneer een kaart wordt ingelezen door de urne worden de volgende controles door de urnesoftware verricht :

– de kaart moet vooraf zijn geïnitialiseerd op de pc van de voorzitter van het stembureau;

– de CRC van de kaart wordt herberekend op de pc van de voorzitter van het stembureau;

– de stem moet ofwel niet uitgebracht (ongebruikt in een stemmachine), ofwel blanco zijn, ofwel overeenkomen met de lijsten en kandidaten die gelden in dat stembureau.

Als aan deze voorwaarden is voldaan, wordt de uitgebrachte stem weggeschreven in een RAM bestand en op diskette (Digivote of Jites in beperkte modus) of in EEPROM (Jites). De plaats van opslag van de stem is willekeurig en niet reproduceerbaar : ze is afhankelijk van het

deuse. Si au moment de son introduction dans la valideuse, la carte n'est pas vierge, la valideuse la rejette et émet un signal sonore (sauf si les données correspondent à une ancienne élection - auquel cas elle est initialisée).

4.1.5.4.3. Logiciel des machines à voter

La lecture des codes sources permet de constater les éléments suivants :

– La machine à voter ne peut être démarrée qu'à l'aide du mot de passe du président du bureau de vote.

– Seules les cartes magnétiques initialisées sur le PC du président peuvent être utilisées sur les machines à voter d'un bureau de vote.

– Après avoir voté, l'électeur peut vérifier son vote en réintroduisant sa carte dans n'importe quelle machine à voter du bureau de vote. Il ne peut plus modifier le vote. Cette vérification ne laisse aucune trace sur la carte. Elle peut être donc répétée autant de fois que souhaité.

– Le vote est supprimé de la mémoire de la machine à voter (remis à zéro) après l'éjection de la carte magnétique. Seule la carte magnétique contient le vote après que la carte ait été retirée de la machine à voter et avant son introduction dans l'urne.

– La carte magnétique contient un CRC (code de contrôle) en plus du vote émis pour permettre à l'urne de vérifier la validité de la piste magnétique. Le vote n'est pas encrypté par manque de place sur la piste.

4.1.5.4.4. Introduction d'une carte à voter dans l'urne

Lorsqu'une carte à voter est introduite dans l'urne, les contrôles suivants sont effectués par le logiciel de l'urne :

– la carte doit avoir été initialisée sur le PC du président du bureau de vote;

– le CRC de la carte est recalculé et doit être égal à celui calculé par la machine à voter;

– le vote doit être soit non émis (carte non introduite dans une machine à voter), soit blanc, soit correspondre aux listes et candidats valables pour le bureau de vote.

Si ces conditions sont remplies, le vote émis sur la carte est enregistré dans un fichier en RAM et sur la disquette (Digivote ou Jites en mode dégradé) ou sur l'EEPROM (Jites). La position d'enregistrement du vote est aléatoire et non reproductible : elle dépend du moment du démarrage

moment van het opstarten van de urne en van het inlezen in de urne van alle voorafgaande stemmen. De stem wordt geëncrypteerd met een sleutel bestaand uit drie onafhankelijke sleutels alvorens ze wordt weggeschreven.

Bij de registratie van een stem in de urne worden er verschillende controles uitgevoerd :

– Verschillende tellers worden in geheugen verdrievoudigd en systematisch vergeleken.

– De stemmen in het geheugen worden vergeleken met die in EEPROM (Jites) of op de diskette (Digivote). In geval van tegenstrijdigheid is de inhoud van het geheugen doorslaggevend.

Als een van de hierboven vermelde problemen zich voordoet of als er een probleem is bij de registratie van de stemmen, gaat de urne over in beperkte modus : zij gaat door met het controleren van de stemmen maar slaat ze niet verder op (behalve bij het Jitessysteem). De stemmen zullen dan opnieuw moeten worden ingelezen in een nieuwe urne na het sluiten van het stembureau.

Men heeft vastgesteld dat de duur van invoering van een kaart in de Digivote stembussen 8 seconden kan duren. Dit zou sneller moeten kunnen.

In geval van tegenstrijdigheid tussen de versie van de stemming in RAM en op EEPROM of de diskette, beschouwt het programma het bestand in RAM als juist. Hij vervangt dan de file op de diskette door deze uit de RAM. Wij menen dat deze manier van handelen hachelijk is want er is geen garantie dat de fout zich niet in het geheugen bevindt. De overstap naar beperkte modus lijkt ons in dit geval aangewezen.

4.1.5.4.5. Afsluiten van de stembus en de stemverrichtingen

Wanneer alle stemverrichtingen zijn afgelopen en alle kaarten in de urne zijn ingebracht, sluit de voorzitter de stembus af. Om te kunnen afsluiten moet hetzelfde paswoord als bij het opstarten worden gebruikt.

De bestanden met de versleutelde stemmen in het geheugen (RAM) worden vergeleken met die in EEPROM (Jites) of op de diskette (Digivote). In geval van verschil sluit het systeem niet af, laat een bericht verschijnen en gaat over in een « loop ».

Als de twee bestanden identiek zijn wordt de totalisatie in een bestand in RAM uitgevoerd. Dit bestand en het bestand met de stemmen wordt vervolgens versleuteld met een Rijndaelalgoritme en gekopieerd op diskette. De diskette wordt digitaal gehandtekend. Het programma vraagt ook de tweede en daarna de derde diskette in te brengen,

de l'urne et du moment de l'introduction dans l'urne de tous les votes précédents. Le vote est crypté par une combinaison de trois clés indépendantes avant son sauvetage.

Différents contrôles sont effectués à chaque enregistrement d'un vote par l'urne :

– Plusieurs compteurs sont triplés en mémoire et sont systématiquement comparés.

– Une comparaison entre le contenu des votes en mémoire et sur l'EEPROM (Jites) ou la disquette (Digivote) est effectuée. En cas de discordance, le contenu de la mémoire prévaut.

Si un des problèmes énoncés ci-dessus se produit ou si un problème d'enregistrement des votes survient, l'urne passe dans un mode dit « dégradé » : elle continue à vérifier et à accepter les votes valables mais ne mémorise plus les votes (sauf le cas des systèmes Jites). Les votes devront alors être réintroduits dans une nouvelle urne après la fermeture du bureau de vote.

Il a été constaté que la durée d'introduction d'une carte dans les urnes Digivote peut atteindre 8 secondes, ce qui devrait être amélioré.

En cas de discordance entre la version des votes RAM et sur l'EEPROM ou sur la disquette, le programme considère le fichier en RAM comme correct. Il remplace alors le fichier sur la disquette par celui en RAM. Nous estimons que cette manière de procéder est téméraire car il n'y a aucune garantie que l'erreur ne se situe pas en mémoire. Le passage en mode dégradé nous semble dans ce cas plus adéquat.

4.1.5.4.5. Clôture de l'urne et des opérations de vote

Lorsque les opérations de votes sont terminées et toutes les cartes introduites dans l'urne, il est procédé à la clôture de l'urne. Le même mot de passe que celui utilisé à l'initialisation du bureau de vote doit être introduit pour pouvoir commencer la clôture.

Les fichiers contenant tous les votes cryptés en mémoire et sur l'EEPROM (Jites) ou sur la disquette (Digivote) sont alors comparés. En cas de différence, le système ne clôture pas, affiche un message et se met en boucle.

Si les deux fichiers sont identiques, la totalisation est effectuée dans un fichier en RAM. Ce fichier de résultat et le fichier des votes sont alors cryptés par l'algorithme Rijndael et copiés sur la disquette. La disquette est alors signée de façon digitale. Le programme demande d'introduire la deuxième puis la troisième disquette sur lesquelles

waarop ook de geëncrypteerde bestanden met de stemmen en de resultaten worden geschreven. Ook deze diskettes worden gehandtekend.

Het originele bestand met de geëncrypteerde stemmen wordt logisch maar niet fysiek gewist. Het is dus mogelijk om dit oorspronkelijke bestand terug te vinden met behulp van specifieke software (undelete).

Het verdient aanbeveling om alle wisprocedures van magnetische media fysiek uit te voeren : alle informatie dient effectief overschreven te worden.

4.1.5.5. Totalisatieprogramma

De broncode van de totalisatie werd summier bekeken en er zijn geen speciale opmerkingen.

Het college heeft de voorkeur gegeven aan het hertotaliseren van de resultaten in parallel met de totalisatie uitgevoerd door de gemeentes. Deze hertotalisatie is uitgevoerd met een programma dat door het college zelf werd ontwikkeld.

4.1.5.6. Veiligheid : Beschouwingen in verband met de softwarecode

Het voornaamste mechanisme waar alle software veiligheid op gebaseerd is, is het algoritme van Rijndael, zowel voor de encryptie als voor de « hashing » functies voor de parameters van versleuteling (Message Authentication Code). Hoewel de code op een vrij modulaire wijze is geschreven, verdient het aanbeveling om te waarborgen dat in geval van nood het algoritme van Rijndael op eenvoudige wijze kan vervangen worden door een ander algoritme.

De software zou moeten ontworpen en geschreven worden zodanig dat « hashing » en encryptie algoritmen snel en gemakkelijk kunnen worden vervangen. Het zou ook mogelijk moeten zijn om op eenvoudige wijze verschillende algoritmen in te bouwen om berichten te encrypteren of via « authenticatie » te identificeren (in de huidige versie van de software gebeuren de twee operaties uiteindelijk via éénzelfde algoritme van Rijndael).

Op de magneetkaarten wordt een foutcorrectiecode gebruikt om de integriteit van de stemmen die er op geregistreerd worden te waarborgen. Hiervoor berekent de functie « calcul_crc » een MAC (Message Authentication Code), dat wil zeggen een robuuste encryptie bewerking; deze waarde wordt vervolgens ingekort op twee bytes door het iteratief toepassen van een « exclusieve or »-bewerking op de oorspronkelijke MAC bytes. De opgeleverde waarde, bestaande uit twee bytes, zijn minder robuust dan de oorspronkelijke MAC code, en het risico van « collisions » (het feit dat verschillende stemmen aanleiding geven tot

sont également écrits les fichiers de votes et de résultats cryptés. Ces disquettes sont également signées.

Le fichier d'origine contenant les votes cryptés est détruit logiquement mais pas physiquement. Il est donc possible de récupérer ce fichier d'origine au moyen d'un logiciel adapté (undelete).

De manière générale, il est recommandé de procéder à la destruction physique des fichiers effacés.

4.1.5.5. Logiciel de totalisation

Le code source a été survolé et il n'y a pas de remarques particulières.

Le collège a préféré effectuer une totalisation parallèle à celle des communes. Cette retotalisation a été effectuée à l'aide d'un programme développé par le collège.

4.1.5.6. Sécurité : Considérations liées au code des logiciels

L'outil principal sur lequel se base toute la sécurité des logiciels est l'algorithme Rijndael, que ce soit pour les opérations de chiffrement ou pour la réalisation de fonctions de hachage paramétrées par des clés (Message Authentication Code). Si une certaines modularité apparaît dans la manière dont le code a été écrit, il serait utile de s'assurer que, en cas de nécessité, l'algorithme Rijndael puisse être remplacé le plus facilement possible par un autre algorithme.

Les logiciels devraient être écrits de manière à permettre le remplacement des algorithmes de chiffrement et de hachage le plus aisément et le plus rapidement possible. Il devrait aussi être possible de pouvoir aisément mettre en place des algorithmes distincts pour chiffrer ou pour « authentifier » les messages (dans la version actuelle des logiciels, ces deux opérations dépendent finalement du même algorithme Rijndael).

Un code correcteur d'erreur est utilisé sur les cartes magnétiques afin de garantir l'intégrité des votes qui y sont inscrits. Pour ce faire, la fonction « clacul_crc » réalise le calcul d'un MAC (message authentication code), qui est une opération cryptographiquement robuste. Cette valeur est par la suite réduite à deux octets par la réalisation itérative d'un « ou exclusif » sur les différents octets du MAC initialement calculé. Les deux octets ainsi obtenus ne présentent plus la même robustesse que le MAC original, le risque de collisions (à savoir que deux votes distincts produisent les mêmes deux octets) y est sensiblement plus

dezelfde code) is gevoelig groter. Een dergelijke procedure lijkt nodig in het licht van de beperking op beschikbare plaats op de gebruikte magneetkaarten.

De verschillende encryptiebewerkingen gebruikt binnen de kiessoftware vereisen het gebruik van « random » getallen. Het niveau van veiligheid aangeboden door de gebruikte encryptietechnieken hangt rechtstreeks af van de kwaliteit van willekeurig te zijn van deze « random » getallen (het gebruik van een rij van getallen die voorspelbaar is of waarvan de lengte van de rij te kort is, kan aanleiding geven tot een veiligheidsrisico). De software die instaat voor de voorbereiding van de diskettes voor de kiesbureaus berekent en gebruikt dergelijke « random » getallen ten einde encryptiesleutels te bepalen, alsook MAC sleutels en de gebruikte startwaarden (IV, « initial value »). De veiligheid van de onderliggende encryptie primitieven (encryptie en MAC) hangt dus rechtstreeks af van de werkelijke willekeurigheid van de waarden die dienen voor de aanmaak van deze sleutels. Binnen de software voor de kiesverrichtingen worden (pseudo-) willekeurige getallen gegenereerd door een functie uit het « SQLWindows » systeem genaamd « SalNumberRandom ».

Er zou een analyse moeten uitgevoerd worden over de manier om best « random » getallen en initiële waarden te genereren.

Bij het insteken in de urne van een magneetkaart met daarop de stem van de kiezer wordt deze overgeschreven zowel naar de diskette als naar het geheugen (als « ramdrive » geconfigureerd) in het bestand « FE_DSK ». De stem wordt daarin geëncrypteerd via een functie « encrypt_decrypt » uit het bestand « VARIABLE.C ». Deze encryptie procedure bestaat uit de toepassing van de voorzitter, de vier lettertekens eigen aan de verkiezing en de positie waarop de stem in het geheugen genoteerd wordt. Bij de sluiting van het bureau wordt het « FE_DSK » bestand geëncrypteerd via het Rijndael algoritme, waarna het oorspronkelijke bestand wordt gewist.

De encryptering die gebruikt wordt voor het versleutelen van de individuele stemmen op het « FE_DSK » bestand kan eventueel niet robuust blijken (het lijkt ons ingegeven door het schema van Vernam, maar zonder waarborg over de kwaliteit van het willekeurige karakter van de gebruikte sleutel).

Er wordt aanbevolen om te waken over de robuustheid van de encryptering van de individuele stemmen. Ten einde te vermijden dat er een « vals » bestand « FE_DSK » wordt aangemaakt is het tevens te vermijden dat noch de software, noch het paswoord te vroeg in de handen van de voorzitter van het kiesbureau terecht komen. Om dat te verwezenlijken zouden het paswoord en de diskettes met de verkiezingssoftware niet tegelijkertijd mogen afgeleverd worden aan de voorzitters.

important. Une telle procédure semble être rendue nécessaire par le peu d'espace disponible sur les cartes magnétiques.

Différentes opérations cryptographiques réalisées par les logiciels nécessitent des nombres aléatoires. Le niveau de sécurité offert pas ces opérations cryptographiques dépend aussi de la qualité des nombres aléatoires produits (l'usage d'une séquence de nombres qui serait prédictible ou dont la taille de la séquence serait trop courte induirait un risque sécuritaire). Le logiciel de préparation des disquettes de bureaux de vote crée et utilise de tels nombres aléatoires afin de produire des clés de chiffrement, les clés pour les MAC ainsi que les valeurs initiales (IV, « initial value ») utilisées. La sécurité des primitives cryptographiques sous-jacentes (chiffrement et MAC) dépend donc directement de la qualité des valeurs aléatoires utilisées pour créer ces clés. Au sein des logiciels des élections, les nombres (pseudo-)aléatoire sont générés par une fonction du langage « SQLWindows » nommée « SalNumberRandom ».

Une analyse quant à la manière de générer les nombres aléatoires nécessaires à la création des clés cryptographiques et des valeurs initiales devrait être réalisée.

Lors de l'introduction dans l'urne d'une carte magnétique contenant le vote d'un électeur, le vote est écrit sur disquette et en mémoire (ramdrive) dans le fichier FE_DSK. Le vote y est chiffré au moyen de la fonction « encrypt_decrypt » du fichier « VARIABLE.C ». Cette procédure de chiffrement consiste en la réalisation d'un « ou » exclusif entre le vote et une clé composée à partir du mot de passe du président, des quatre caractères propres à l'élection et de la position à laquelle le vote est inséré dans la mémoire. A la clôture du bureau, le fichier FE_DSK est chiffré au moyen de l'algorithme de chiffrement Rijndael; la version du fichier avant son chiffrement est effacée.

Le chiffrement utilisé pour chiffrer les votes individuels sur FE_DSK peut ne pas être robuste (il nous semble inspiré du schéma de Vernam mais sans garantie quant à la qualité du caractère aléatoire de la clé utilisée).

Il est recommandé de s'assurer de la robustesse de la méthode de chiffrement des votes individuels. Il est aussi nécessaire, afin d'éviter de pouvoir construire un « faux » fichier FE_DSK de ne pas concentrer dans les mains des présidents de bureaux de vote, trop longtemps avant le jour des élections, à la fois son mot de passe et les logiciels des élections. Pour ce faire, le mot de passe ne devrait pas être fourni aux présidents de bureaux de vote en même temps que les disquettes contenant les logiciels des élections.

4.1.5.7. Kwaliteit van de broncode

De software die gebruikt wordt is een mix van, onder andere, C en C++ code en deze code beantwoordt niet overal strikt aan de standaarden van de taal. Dit verhindert het gebruik van vele automatische analyse programma's voor broncode. Code analyse is wel kunnen uitgevoerd worden door « flawfinder », een programma dat eventuele veiligheidsproblemen in programma code aangeeft. De resultaten hiervan zijn dat in de code op vele plaatsen zich potentieel veiligheidsproblemen door « buffer overflows » bevinden. Gezien de aard van de software en het systeem : een single tasking systeem met strikt gekende inputlimieten, vormt dit echter geen probleem.

Algemeen heeft de code een lage kwaliteit met betrekking tot leesbaarheid en onderhoudbaarheid. Een niet-exhaustieve lijst van mindere elementen is de volgende :

– Er wordt misbruik gemaakt van globale variabelen als functieparameters.

– De code bevat algemeen te weinig commentaar, en waar er commentaar is, is deze grotendeels waardeloos of verouderd.

– Er is sprake van copy-paste hergebruik van functies over verschillende files met aanpassen van de parameters.

– De urne software krijgt bij het opstarten een optie meegegeven, deze optie dient tot niets.

– Bij lezing van de verschillende programma's blijkt dat codebestanden met eenzelfde naam op verschillende plaatsen in gebruik zijn, hoewel hun inhoud verschilt. Zo vinden we bijvoorbeeld ondermeer een bestand genaamd « API-FST.C » zowel in de software voor de urne als in de software voor de kiesmachines. Er blijken verschillen in deze verschillende bestanden, hoewel in alle gevallen « version 2.91 (September 2001) » in de hoofding vermeld wordt. Ook stellen we soms vrij belangrijke verschillen vast tussen de verschillende plaatsen waar een codebestand genaamd « RIJN2.C » gebruikt wordt; hetzelfde geldt voor een codebestand genaamd « FLOPPY.C ».

In het algemeen kan gesteld worden dat de code een lage verstaanbaarheid heeft, wat het werk van het college met betrekking tot de studie van de code significant bemoeilijkt.

Er moeten correcte methodologische regels van goed gebruik opgelegd worden tijdens het ontwerp en verwezenlijking van de software.

4.1.6. Simulatie van de twee types stembureau

Op 28 september 2006 werden 2 type bureaus opgesteld die de experten moesten toelaten de definitieve versie van

4.1.5.7. Qualité du code source

Le software qui est utilisé est un mélange entre autres de C et de C++ et ce code ne répond pas toujours de manière stricte aux standards de ce langage. Ceci empêche l'utilisation de la plupart des outils d'analyse automatique de code source. L'analyse du code a pu être effectuée à l'aide du programme « flawfinder » qui permet de révéler d'éventuels problèmes de sécurité. Le résultat de cette analyse montre qu'il existe à de nombreux endroits des risques potentiels de sécurité liés aux « buffer overflows ». Vu le type de logiciel et de système, à savoir un système monotâche avec des inputs parfaitement connus et limités, cela ne constitue pas un problème réel.

De façon générale le code est de pauvre qualité en ce qui concerne la lisibilité et la facilité de maintenance. Une liste non exhaustive des faiblesses suit :

– Il est fait usage abusif des variables globales comme paramètres de fonctions.

– Le code contient trop peu de commentaires, et quand il y en a, ils n'apportent généralement pas d'information ou sont obsolètes.

– Il est fait usage de copy-paste de fonctions à travers différents fichiers avec adaptation des paramètres.

– Le logiciel d'urne à des paramètres de démarrage qui sont sans objet.

– A la lecture des différents programmes, il apparaît que des fichiers de codes portant un même nom apparaissent à plusieurs endroits alors que ces fichiers ont en fait des contenus qui peuvent différer. Par exemple, on retrouve un fichier nommé « API-FST.C », entre autres, dans le logiciel der urnes et dans le logiciel des machines à voter; des différences apparaissent dans le contenu de ces fichiers alors qu'ils indiquent touts la même mention « version 2.91 (septembre 2001) ». De la même manière, on note des différences parfois importantes entre deus occurrences d'un fichier de code nommé « RIJN2.C » ainsi qu'entre différentes occurrences d'un fichier de code nommé « FLOPPY.C ».

De façon générale le code est difficilement compréhensible, ce qui a compliqué considérablement le travail du collège concernant l'étude du code.

Des règles méthodologiques et de bonnes pratiques pour l'écriture et la conception du code des logiciels devraient être imposées.

4.1.6. Simulation des deux types de bureaux de vote

Le 28 septembre 2006, deux bureaux type ont été installés pour permettre aux experts de tester en conditions

de software in reële omstandigheden te testen. Het MBHG had hiervoor een set diskettes gegenereerd van een reëel stembureau, namelijk Koekelberg 2. Het spreekt voor zich dat het MBHG dit stembureau volledig opnieuw heeft gegenereerd na deze testen.

Het doel is zich er van te vergewissen dat :

– De stem juist wordt weggeschreven op de magneetkaart;

– Het inlezen van de magneetkaart in de urne verandert de inhoud van de kaart niet;

– De totalisatie van de urne is juist;

– De software werkt op dezelfde manier onafhankelijk van het materiaal.

4.1.6.1. Digivote

Een Digivote stembureau werd als eerste getest.

Allereerst werd de diagnosediskette uitgetest. Hierbij werd een kopie van de diagnosediskette voor en na de test genomen en vergeleken. Drie files werden inderdaad op de diskette geschreven met de resultaten van de uitgevoerde testen. Bij de diagnostiek van de stemmachine moest telkens de urne aan de stemmachine gekoppeld worden.

Na de diagnose werd een stembureau (PC voorzitter en één stemmachine) opgestart. Verschillende testen werden uitgevoerd en de verwachte reactie van de PC werd vastgesteld.

Het college heeft een twintigtal stemmen uitgebracht. Na het afsluiten van de urne, werd het resultaat gedecrypteerd en werden de resultaten vergeleken met de resultaten van een manuele telling. De resultaten kwamen overéén.

4.1.6.2. Jites

Diezelfde dag werd een Jites stembureau opgestart met dezelfde set diskettes (urne en stemmachine). Opnieuw reageerde beide conform de verwachtingen.

4.1.7. Handleiding en opleiding van de voorzitters van de stembureaus

Slechts enkele dagen voor de verkiezingen voorzag het MBHG de gemeentes van de volledige « stembureauhandleiding » bestemd voor de voorzitters van de stembureaus. De gemeentes zorgden echter voor de opleiding van de voorzitters in de weken voor de verkiezingen; dus voor het verschijnen van de definitieve versie van de officiële handleiding.

réelles la version définitive du logiciel. Le MRBC a généré à cette fin le jeu de disquettes pour le bureau 2 de Koekelberg. Il va de soi que le MRBC a généré une version neuve de ce bureau après les tests.

L'objectif est de s'assurer que :

– le vote est bien transcrit sur la carte magnétique;

– le passage de la carte magnétique dans l'urne ne l'altère pas;

– la totalisation de l'urne est correcte;

– le logiciel fonctionne de la même manière indépendamment du matériel.

4.1.6.1. Digivote

Un bureau Digivote a d'abord été testé.

La disquette de diagnostic a tout d'abord été étudiée. Une copie de cette disquette a été prise et comparée avant et après les tests. Trois fichiers ont été écrits sur la disquette avec les résultats des tests effectués. Lors du diagnostic des machines à voter, il a fallu à chaque fois connecter une urne à la machine à voter.

Après le diagnostic, un bureau de vote (une machine du président et une machine à voter) a été démarré. Plusieurs tests ont été effectués et la réaction du PC a été constatée.

Le collège a émis une vingtaine de votes. Après clôture de l'urne, les résultats ont été décryptés et ils ont été comparés à ceux d'une totalisation manuelle. Les résultats correspondaient.

4.1.6.2. Jites

Le même jour, un bureau de vote Jites a été démarré avec le même set de disquettes (urne et machine à voter). A nouveau les deux ont réagi conformément aux attentes.

4.1.7. Manuels et formation des présidents des bureaux de vote

Quelques jours seulement avant les élections, le MRBC a fourni aux communes la version définitive et complète du « manuel bureau de vote » destiné aux présidents des bureaux de vote. La formation des présidents de bureaux a quant à elle été assurée par les services des communes dans les semaines précédant les élections, donc avant la parution de la version définitive du manuel officiel.

De handleiding is volledig maar vrij moeilijk en bevat enkele minder belangrijke fouten.

Door de laattijdige overhandiging van de handleiding door het MBHG hebben sommige gemeentes gezorgd voor een eigen « stembureauhandleiding ». Deze handleiding bevatte niet altijd noch de laatste gegevens, noch sommige gegevens betreffende de veiligheidsprocedures.

In het bijzonder voegde, om veiligheidsredenen, het MBHG de foto's van de deskundigen van het college toe. Niet alle voorzitters van de stembureaus beschikten over dit document. In hetzelfde document werd ook de rol van het college (te summier) belicht en de voorzitters gevraagd aan de vragen van de deskundigen van het college te voldoen. Bij afwezigheid van deze informatie vormde de toegang of de controle in bepaalde bureaus problemen.

Daarenboven lijkt dat bepaalde gemeentes al op voorhand beslist hadden hun eigen instructies voor de stembureaus op te leggen en dit in overtreding met de procedures die de geautomatiseerde stemming regelen.

Er zou meer zorg moeten worden gedragen bij het opstellen van het handboek voor de voorzitters. Dit zou minstens twee maanden voor de verkiezingen beëindigd moeten worden zo dat alle voorzitters over dezelfde informatie beschikken.

Daarnaast moeten de gemeentes de officiële procedures naleven en ervoor zorgen dat die worden gevolgd.

4.1.8. Diagnose en installatie van het materiaal in de gemeentes

De dag voor de verkiezingen is het college getuige geweest van de installatie en de tests van goede werking in enkele stembureaus : bureaus 14, 15, 16, 17 en 23 te Brussel, bureaus 13, 20 tot en met 24 en 48 in Elsene, bureau 19 in Sint-Pieters-Woluwe en de bureaus 10, en 13 in Schaarbeek.

Kopieën van de diagnosediskettes werden genomen voor controle. De vergelijking tussen de diagnosediskettes en de geanalyseerde en de opnieuw op onafhankelijke wijze gecompileerde programmatuur (zie § 4, 1.3.2) door het college toont aan dat het om dezelfde code gaat.

Het is nodig om eraan te herinneren dat de fysieke veiligheid van de machines belangrijk is om de goede werking van de verrichtingen van dag van de verkiezingen te garanderen. Het college heeft vastgesteld dat dit punt in bepaalde gemeentes werd verwaarloost en dat dit aspect zou moeten verbeterd worden.

De façon générale, le manuel, bien que complet, est assez ardu. Il présente également certaines erreurs mineures.

La remise tardive du manuel par le MRBC a eu pour conséquence que certaines communes ont fourni leur propre manuel aux présidents des bureaux de vote, manuel qui ne contenait ni les informations de dernière minute, ni certaines informations concernant les procédures de sécurité.

En particulier, le MRBC a ajouté la photo des experts du collège pour des raisons de sécurité. Ce document n'est pas parvenu à tous les présidents de bureau de vote. De même, le manuel indiquait (trop sommairement) le rôle du collège et invitait les présidents à répondre aux demandes des experts du collège. En l'absence de ces information, l'accès ou le contrôle dans certains bureaux a posé problème.

Par ailleurs, il semble que certaines communes avaient décidé d'emblée d'imposer leurs propres instructions aux bureaux de vote et ce en violation des procédures régissant le vote automatisé.

Un plus grand soin devrait être apporté à la rédaction du manuel des présidents de bureau de vote. Celui-ci devrait être terminé au moins deux mois avant les élections de façon à ce que tous les présidents disposent des même informations.

De plus, les communes doivent veiller à respecter et à faire respecter les procédures officielles.

4.1.8. Diagnostic et installation du matériel dans les communes

La veille de l'élection, le collège a assisté à l'installation et aux tests de bon fonctionnement de quelques bureaux de vote : Bruxelles, bureaux 14, 15, 16, 17 et 23, Ixelles, bureaux 13, 20 à 24 et 48, Woluwe-Saint-Pierre bureau 19 et Schaerbeek, bureaux 10 et 13.

Des copies des disquettes de diagnostic ont été prises à des fins de contrôle. La comparaison entre les disquettes de diagnostic et le programme analysé et recompilé de façon indépendante (voir § 4.1.3.2.) par le collège montre qu'il s'agit du même code.

Il convient de rappeler que la sécurité physique des machines revêt une importance réelle pour garantir le bon fonctionnement des opérations le jour des élections. Les constatations du collège dans certaines communes montrent que cet aspect est négligé et devrait être amélioré.

4.2. Vaststellingen op de dag van de verkiezingen

4.2.1. Controle in de stembureaus

In alle 19 Brusselse gemeentes werden controles uitgevoerd. In alle gecontroleerde stembureaus werden kopieën genomen van de diskettes met de gebruikte software. Deze kopieën werden meegenomen voor verder analyse. Hieruit is gebleken dat ook de uitvoeringscodes, gebruikt op de verkiezingsdag, binair identiek zijn aan die gegenereerd tijdens de referentiecompilatie (cf. § 4.1.3.3) en waarvan de broncode werd geanalyseerd door het college van deskundigen.

In alle bureaus hebben de deskundigen tevens referentiestemmen uitgebracht en op een verschillende stemmachine bekeken. Dit laatste gebeurde samen met een getuige. In alle gevallen werden deze referentiestemmen correct weergegeven.

In de volgende stembureaus werden controles uitgevoerd :

4.2. Constatations le jour des élections

4.2.1. Contrôles dans les bureaux de vote

Des contrôles ont été effectués dans les dix-neuf communes de la Région. Dans chaque bureau contrôlé, une copie de la disquette en cours d'utilisation a été prise. Ces copies ont été emportées pour être analysées. Il s'est avéré que les programmes exécutés le jour des élections étaient identiques à ceux générés lors de la compilation de référence (voir § 4.1.3.3.) et dont le code source avait été analysé par le collège des experts.

Dans tous les bureaux contrôlés, les experts ont également émis un vote de référence en présence d'un assesseur et vérifié son contenu sur une autre machine à voter. Dans tous les cas, les votes de référence se sont avérés corrects.

Liste des bureaux contrôlés

Gemeente – Commune	Nr. bureau – Bureau	Kaarten – Nombre de votes		Type machine – Système
Anderlecht	23	1	OK	Digivote
	28	1	OK	Digivote
	57	1	OK	Digivote
Oudergem/Auderghem	11	1	OK	Digivote
	13	2	OK	Digivote
	18	1	OK	Digivote
	20	2	OK	Digivote
Sint-Agatha-Berchem/Berchem-Ste-Agathe	2	2	OK	Digivote
	3	2	OK	Digivote
	9	2	OK	Digivote
	11	1	OK	Digivote
Brussel/Bruxelles	21	1	OK	Digivote
	22	1	OK	Digivote
	23	2	OK	Digivote
Etterbeek	13	1	OK	Jites
	14	1	OK	Jites
	15	1	OK	Jites
	16	2	OK	Jites
	26	1	OK	Jites
	27	1	OK	Jites
Evere	2	1	OK	Digivote
	5	2	OK	Digivote
	10	1	OK	Digivote
	11	1	OK	Digivote
	12	1	OK	Digivote
	13	1	OK	Digivote

Vorst/Forest	4	2	OK	Digivote
	5	2	OK	Digivote
Ganshoren	10	1	OK	Digivote
	15	1	OK	Digivote
Elsene/Ixelles	1	1	OK	Digivote
	12	1	OK	Digivote
Jette	18	2	OK	Digivote
	19	2	OK	Digivote
	20	2	OK	Digivote
	21	2	OK	Digivote
	22	2	OK	Digivote
	23	2	OK	Digivote
Koekelberg	1	1	OK	Digivote
	2	2	OK	Digivote
	6	2	OK	Digivote
	7	2	OK	Digivote
Molenbeek	26	1	OK	Digivote
	32	1	OK	Digivote
	48	1	OK	Digivote
Schaarbeek/Schaerbeek	8	2	OK	Digivote
	9	2	OK	Digivote
St-Gillis/St-Gilles	2	1	OK	Digivote
	3	1	OK	Digivote
	4	1	OK	Digivote
	5	1	OK	Digivote
	6	1	OK	Digivote
	19	1	OK	Digivote
Sint-Joost-ten-Node/Saint-Josse-ten-Noode	9	1	OK	Jites
	10	1	OK	Jites
Ukkel/Uccle	17	3	OK	Digivote
	18	2	OK	Digivote
Watermaal-Bosvoorde/Watermael-Boitsfort	1	1	OK	Digivote
	3	1	OK	Digivote
	23	1	OK	Digivote
	24	1	OK	Digivote
Sint-Lambrechts-Woluwe/Woluwe-Saint-Lambert	8	2	OK	Jites
	9	2	OK	Jites
	10	2	OK	Jites
Sint-Pieters-Woluwe/Woluwe-Saint-Pierre	8	2	OK	Jites
	9	2	OK	Jites
	22	2	OK	Jites
	25	2	OK	Jites

Dus in totaal 68 bureaus en 99 referentiestemmen.

Cela fait au total 68 bureaux et 99 votes de référence.

4.2.2. Controle in de totalisatiebureaus

De leden van het college zijn de avond van de verkiezingen in de volgende bureaus langs geweest :

– Sint-Pieters-Woluwe

– Oudergem

– Schaarbeek

– Sint-Joost-ten-Node

– Anderlecht

De deskundigen hebben kopieën genomen van de diskettes van die stembureaus. Deze zijn later geanalyseerd.

In Schaarbeek waren de experten aanwezig wanneer een urne moest worden herteld.

Verder werden er geen incidenten vastgesteld.

4.2.3. Organisatie van de stembureaus en de richtlijnen aan de voorzitters van deze bureaus – Vaststellingen in de stembureaus

De deskundigen hebben de dag van de verkiezingen vastgesteld dat de organisatie van de stembureaus meestal goed was. Enkele minder goed georganiseerde bureaus zijn wel met vertraging opgestart. Andere belangrijke vertragingen (1h30 à 2h00) zijn te wijten aan een trage interventie van de helpdesktechnici bij defecten.

Het is ook gebleken dat sommige voorzitters en verantwoordelijken van de gemeentes slecht waren geïnformeerd over de te volgen procedures :

– Bij het openen van enkele stembureaus bleek dat de veiligheidsvoorschriften niet werden gerespecteerd : stemmachines en voorzittersmachines waren opgestart voor de samenstelling van het bureau. Dit is tegenstrijdig met de veiligheidsregels, duidelijk aangegeven in de handleiding : niets kan verzekeren dat de voorzitter de verzegelde enveloppen niet voor de verkiezingen opende. Daarnaast werd er, ondanks de uitdrukkelijke richtlijnen in de laatste versie van de handleiding van het MBHG, door meerdere voorzitters systematisch blanco gestemd bij het nemen van de referentiestemmen. Daardoor wordt het nut van de referentiestemmen bij een mogelijke verdenking van fraude tijdens de stembusgang teniet gedaan.

– De voorzitters van de stembureaus en de verantwoordelijken van de gemeentes waren zeer slecht geïnformeerd over de rol en het doel van de door het college uitgevoerde controles. Dit is grotendeels te wijten aan het

4.2.2. Contrôles dans les bureaux de totalisation

Les membres du collège se sont rendus dans les bureaux suivants le soir des élections :

– Woluwe-Saint-Pierre

– Auderghem

– Schaerbeek

– Saint-Josse-tenNoode

– Anderlecht

Les experts ont pris copie des disquettes de ces bureaux pour analyse ultérieure.

A Schaerbeek, les experts ont assisté au recomptage d'une urne.

Aucun incident particulier n' été constaté.

4.2.3. Organisation des bureaux de vote et instruction aux président de ces bureaux – Constatations dans les bureaux de vote

Le jour des élections, les experts ont constaté que dans l'ensemble, l'organisation des bureaux était bonne. Certains bureaux moins bien organisés ont démarré avec du retard. D'autres retards plus importants (de 1h30 à 2h00) sont à imputer à la lenteur de l'intervention des techniciens du helpdesk suite à des pannes matérielles.

Il est également apparu que certains président et responsables des communes semblaient mal informés sur les procédures :

– Lors de l'ouverture de certains bureaux de vote, il a été constaté que les directives de sécurité n'étaient pas respectées : des machines à voter et des machines de présidents ont été démarrées par le président seul, avant la constitution du bureau. Ceci est en contradiction avec les règles de sécurité pourtant clairement édictées dans le manuel : rien ne permet d'assurer que les enveloppes scellées n'ont pas été ouvertes par le président avant le jour de l'élection. De plus, malgré les instructions explicites dans la dernière version du manuel du MRBC, plusieurs présidents de bureaux de vote ont encore émis systématiquement des votes blancs comme votes de référence. Cette façon de procéder enlève toute utilité à ces votes de référence en cas de suspicion de fraude pendant le scrutin.

– Les présidents des bureaux de vote et les responsables communaux étaient très mal informés sur le rôle et l'objectif des contrôles effectués par les experts. Ceci est en grande partie dû à l'absence et/ou au retard de diffusion

ontbreken en/of te laat verspreiden van de laatste versie van de MBHG handleiding. Daarnaast is er nog steeds geen plaats in het PV om het bezoek van de deskundige en de verrichte controles (referentiestemmen, de meegenomen kaarten en het nemen van de kopieën van diskettes) te noteren. Dit ondanks herhaaldelijk verzoek van het college sinds de verkiezingen van 1999 (het jaar van de eerste geautomatiseerde stemming).

– Het ophalen van de diskettes uit alle bureaus laat zien dat niet alle voorzitters de afsluitingsprocedure juist begrepen : meerdere diskettes waren niet juist afgesloten.

Een vereenvoudigde checklist zou het opvolgen van de procedures kunnen verbeteren.

de la dernière version du manuel du MRBC. Par ailleurs, il n'y a toujours pas dans le PV d'emplacement permettant de noter le passage d'un expert et ses opérations de contrôle (votes de référence, cartes emportées, copies de disquettes); ceci malgré les demandes répétées du collège depuis les élections de 1999 (année du premier contrôle du vote automatisé).

– La récolte des disquettes de tous les bureaux de vote a permis de constater également que tous les présidents n'avaient pas compris la procédure de clôture : plusieurs disquettes n'ont pas été correctement clôturées.

Une check-list simplifiée pourrait améliorer le suivi des procédure.

4.3. Controles uitgevoerd na de dag van de verkiezingen

4.3.1. Verificatie van de referentiestemmen

Op 9 oktober 2006 hebben de deskundigen opnieuw de referentiestemmen genomen in de verschillende stembureaus op 8 oktober gecontroleerd. Alle 99 referentiestemmen werden opnieuw correct weergegeven.

4.3.2. Verificatie van de totalisaties

Vanaf de opening van de totalisatiebureaus de avond van de verkiezingen, en de dagen volgend op de stembusgang, hebben de deskundigen van het college kopieën genomen in alle Brusselse gemeentes van alle diskettes gebruikt bij de totalisatie. Het college ontving ook een kopie van alle totalisatie PV's en van het bestand met de resultaten.

Het college totaliseerde de resultaten van de diskettes met een eigen ontwikkeld programma en vergeleek die met de officiële resultaten.

Het college constateerde dat alle resultaten voor alle gemeentes, alle lijsten en alle kandidaten, bekomen met het eigen programma, dezelfde waren onafhankelijk van het gebruikte totalisatieprogramma.

Het college leidt hier uit af dat het totalisatieprogramma gebruikt de avond van de verkiezingen geen fouten maakte bij het totaliseren van de diskettes afkomstig uit de stembureaus.

4.3. Contrôles effectués après le jour des élections

4.3.1. Vérification des votes de référence

Le 9 octobre 2006, les experts ont revisualisé les votes de référence récoltés dans les bureaux de vote contrôlés le 8 octobre. Les 99 votes de référence se sont révélés corrects.

4.3.2. Vérification des totalisations

Dès l'ouverture des bureaux de totalisations le soir des élections, ainsi que dans les jours qui ont suivi le scrutin, les experts se sont rendus dans toutes les communes de la Région bruxelloise afin de prendre une copie des disquettes en provenance de tous les bureaux de vote et ayant servi à la totalisation. Le collège a également reçu une copie des PV de totalisation ainsi qu'une copie du fichier informatique contenant les résultats.

Au moyen de son propre logiciel, le collège a totalisé tous les résultats des disquettes et les a comparés aux résultats officiels.

Le collège a ainsi pu constater que pour toutes les communes, pour toutes les listes et pour tous les candidats, il arrive, avec un logiciel différent, aux mêmes résultats que le logiciel de totalisation utilisé le soir des élections.

Le collège en déduit que le logiciel de totalisation utilisé le soir des élections n'a commis aucune erreur en totalisant les différentes disquettes en provenance des différents bureaux de vote.

4.3.3. Verificatie van de programma's op de diskettes

4.3.3.1. Diskettes gekopieerd in de stembureaus de dag van de verkiezingen

Bij wijze van steekproef werden in de bezochte stembureaus door de deskundigen kopieën gemaakt van master- en/of backup-diskettes (cf. § 4.2.1). De uitvoerbare bestanden en stuurprogramma's werden vergeleken met de referentiebestanden (cf. § 4.1.3.3). Alle bestanden zijn binair identiek.

Gemeente	Bezochte stembureaus
Anderlecht	23, 28, 57
Oudergem	11, 13, 18, 20
Sint-Agatha-Berchem	2, 3, 9, 11
Brussel	21, 22, 23
Etterbeek	13, 14, 15, 16, 26, 27
Evere	2, 5, 10, 11, 12, 13
Vorst	4, 5
Ganshoren	10, 15
Elsene	1, 12
Jette	18, 19, 20, 21, 22, 23
Koekelberg	1, 2, 6, 7
Molenbeek	26, 32, 48
Schaarbeek	8, 9
St-Gillis	2, 3, 4, 5, 6, 19
Sint-Joost-ten-Node	9, 10
Ukkel	17, 18
Watermaal-Bosvoorde	1, 3, 23, 24
Sint-Lambrechts-Woluwe	8, 9, 10
Sint-Pieters-Woluwe	8, 9, 22, 25

4.3.3.2. Diskettes gekopieerd na de verkiezingen voor totalisatie

In de hoofdtelbureaus werden kopieën genomen van alle diskettes gebruikt bij het berekenen van de totalen. De uitvoerbare bestanden en stuurprogramma's werden vergeleken met de referentiebestanden. Alle bestanden waren binair identiek.

Gemeente	Aantal stembureaus
Sint-Lambrechts-Woluwe	33
Ukkel	51
Jette	29
Evere	26
Brussel	95
Molenbeek	51
Vorst	40
Etterbeek	29
Anderlecht	61
Schaarbeek	70
Sint-Pieters-Woluwe	26

4.3.3. Vérification des exécutables présents sur les disquettes

4.3.3.1. Disquettes copiées dans les bureaux de vote le jour des élections

A titre de coup de sonde, les experts ont pris copie des disquettes master et/ou backup dans les bureaux de vote contrôlés le jour des élections (voir § 4.2.1.). Les fichiers exécutables et le système d'exploitation ont été comparés avec ceux de référence (voir § 4.1.3.3.). Tous les fichiers se sont révélés identiques.

Commune	Bureaux de vote
Anderlecht	23, 28, 57
Auderghem	11, 13, 18, 20
Berchem-Sainte-Agathe	2, 3, 9, 11
Bruxelles	21, 22, 23
Etterbeek	13, 14, 15, 16, 26, 27
Evere	2, 5, 10, 11, 12, 13
Forest	4, 5
Ganshoren	10, 15
Ixelles	1, 12
Jette	18, 19, 20, 21, 22, 23
Koekelberg	1, 2, 6, 7
Molenbeek	26, 32, 48
Schaerbeek	8, 9
Saint-Gilles	2, 3, 4, 5, 6, 19
Saint-Josse-ten-Noode	9, 10
Uccle	17, 18
Watermael-Boitsfort	1, 3, 23, 24
Woluwe-Saint-Lambert	8, 9, 10
Woluwe-Saint-Pirre	8, 9, 22, 25

4.3.3.2. Disquettes copiées pour la totalisation après les élections

Une copie de toutes les disquettes ayant servi à la totalisation a été prise dans les bureaux principaux. Les programmes exécutables se trouvant sur ces disquettes se sont avérés identiques à ceux de l'environnement de référence du collège.

Commune	Nombre de bureaux de vote
Woluwe-Saint-Lambert	33
Uccle	51
Jette	29
Evere	26
Bruxelles	95
Molenbeek	51
Forest	40
Etterbeek	29
Anderlecht	61
Schaerbeek	70
Woluwe-Saint-Pirre	26

Watermaal-Bosvoorde	24
Elsene	52
Sint-Joost-ten-Node	12
Sint-Gillis	26
Koekelberg	12
Ganshoren	15
Sint-Agatha-Berchem	16
Oudergem	26

Watermael-Boitsfort	24
Ixelles	52
Saint-Josse-ten-Noode	12
Saint-Gilles	26
Koekelberg	12
Ganshoren	15
Berchem-Sainte-Agathe	16
Auderghem	26

4.4. Verspreiden van de broncode

Het college stelt vast en betreurt dat op het moment van de overhandiging van het verslag, de broncode van de gebruikte software voor deze verkiezingen nog niet werd verspreid. De verantwoordelijken voor de organisatie van de verkiezingen zijn terughoudend om de broncode te verspreiden, omdat bij een mogelijk ingediend beroep er een risico bestaat tot een nieuwe stemming in bepaalde gemeenten.

Het college is van mening dat deze terughoudendheid op technisch niveau niet gerechtvaardigd is en meent dat de broncode vanaf nu zou kunnen worden gepubliceerd, mits de weglating van de 4 lettertekens, uniek voor de verkiezing, gebruikt bij het versleutelen. Het college is voorts van mening dat de huidige lengte van deze code (4 lettertekens) vergroot zou moeten worden om de veiligheid te versterken.

Het college zal, vanaf de publicatie van de broncode, een vervolg op dit verslag overhandigen met daarin de resultaten van de analyse van de overeenstemming tussen die broncode en de broncode gebruikt bij de referentiecompilatie (zie § 4.1.3).

4.4. Diffusion du code source

Le collège constate et regrette qu'au moment de la remise de son rapport, le code source des logiciels utilisés pour ces élections n'ait pas encore été diffusé. Les réticences émises par les responsables de l'organisation des élections pour ne pas diffuser le code source font état de possibles recours introduits et donc d'un risque de devoir procéder à un nouveau scrutin dans certaines communes.

Le collège estime que ces réticences ne se justifient nullement sur le plan technique et est d'avis que les codes sources pourraient être publiés dès à présent, moyennant la suppression d'un code de 4 caractères unique à l'élection et intervenant dans les clés de chiffrement. Le collège est par ailleurs d'avis que la longueur actuelle de ce code (4 caractères) devrait être accrue pour renforcer la sécurité.

Le collège s'engage, dès la publication du code source, à remettre un avenant au présent rapport, reprenant les résultats de l'analyse de la conformité du code source publié avec celui utilisé lors de la compilation de référence (voir § 4.1.3.).

5. Vergelijking met de geautomatiseerde stemprocedure in andere landen

5.1. Verenigde Staten

In de Verenigde Staten is er al aanzienlijke tijd een debat aan de gang over de betrouwbaarheid van de elektronische stemmachines die daar gebruikt worden. We rapporteren hier over een aantal bevindingen gepubliceerd door experts van de universiteit van Princeton inzake computer beveiliging : Ariel J. Feldman, J. Alex Halderman, en Edward W. Felten, onder de titel « Security Analysis of the Diebold AccuVote-TS Voting Machine » op 13 september 2006.

5.1.1. De hardware

De stemmachine die ter discussie staat is de Diebold AccuVote-TS stemmachine, die gebruikt wordt door 10 % van de stemmers in de VS. Deze machine is van het zogenaamde type Direct Recording Electronic (DRE). De uit-

5. Comparaison avec la procédure de vote automatisé dans d'autres pays

5.1. Etats-Unis

Aux Etats-Unis, depuis un certain temps déjà, un débat est en cours au sujet de la fiabilité des machines à voter électroniques utilisées. Nous rapportons ici un certain nombre de constatations concernant la sécurité informatique publiées par les experts de l'université de Princeton : Ariel J. Feldman, J. Alex Halderman et Edward W. Felten, sous le titre « Security Analysis of the Diebold AccuVote-TS Voting Machine » en date du 13 septembre 2006.

5.1.1. Le matériel

La machine à voter qui est l'objet du débat est l'appareil AccuVote-TS qui est utilisée par 10 % des électeurs aux Etats-Unis. Cette machine est du type Recording Electronic direct (DRE). Les votes émis sont, contrairement à ce qui

gebrachte stemmen worden, in tegenstelling tot in België, opgeslagen in het geheugen van de stemmachine zelf, op een geëncrypteerde wijze. Dit geheugen bewaart deze gegevens ook als de machine uitgezet wordt of als de stroom wegvalt. De kiezer wordt, zoals in België een stemkaart overhandigd, maar deze kaart dient enkel om de stemmer toe te laten van een stem uit te brengen. De stem wordt niet opgeslagen op de kaart gebruikt door de kiezer, maar opgeslagen in het geheugen van de machine. Bij het afsluiten van het stembureau produceert elke stemmachine, gebruik makend van een ingebouwde printer, een papieren formulier die zijn resultaten weergeeft. Daarenboven heeft elke machine een verwijderbare geheugenkaart die ook een kopie van de uitgebrachte stemmen bevat, ook op een geëncrypteerde wijze. Deze kaart is beveiligd tegen verwijderen uit de machine door onbevoegden door middel van een slot.

Van belang in deze discussie is hoe de software op de machine up to date gebracht wordt. Het geheugen intern in de stemmachine bevat namelijk, naast de uitgebrachte stemmen, ook de stemsoftware zelf. Om een nieuwe versie van de software te installeren wordt deze op de verwijderbare geheugenkaart gezet, deze kaart in de machine geplaatst, en de machine herstart. Bij het opstarten van de machine verifieert deze of er software aanwezig is op de verwijderbare kaart, en indien dit het geval is wordt deze geïnstalleerd, waarbij oude software overschreven wordt.

5.1.2. De aanval

Bovenstaande onderzoekers zijn er in geslaagd om nieuwe, frauduleuze software te schrijven voor de stemmachine, en deze te installeren op een machine. Deze software gedraagt zich ten opzichte van de kiezer en ten opzichte van de leden van stem- en totalisatiebureaus identiek als de normale software. Het verschil is echter dat deze software gedurende de verkiezingen stemmen steelt van één partij of kandidaat ten voordele van een andere partij of kandidaat. Dit is mogelijk gebruik makend van het feit dat alle reeds uitgebrachte stemmen in het geheugen van de machine zijn opgeslagen. Het feit dat de resultaten geëncrypteerd opgeslagen zijn in het geheugen van de machine en op de verwijderbare geheugenkaart heeft hierbij geen noemenswaardig probleem opgebracht, rapporteren de onderzoekers. Als de verkiezing wordt afgesloten zullen de print-out en de geheugenkaart frauduleuze gegevens bevatten. Daarenboven is na het einde van de verkiezingen het onmogelijk vast te stellen dat er frauduleuze software is gebruikt. Bij het afsluiten van het stembureau verwijdert de frauduleuze software al zijn sporen en is dus niet meer terug te vinden.

Het cruciale punt van de aanval, eens de frauduleuze software geschreven, is deze software te installeren op de stemmachines. Het blijkt dat de mogelijkheid om de software up to date te brengen daarvoor gemakkelijk kan misbruikt worden. De verwijderbare geheugenkaart die

se fait en Belgique., enregistrés sous forme cryptée dans la mémoire de la machine à voter elle-même. Cette mémoire conserve également les données aussi bien dans le cas où la machine est éteinte que dans le cas d'une coupure de courant. L'électeur, comme en Belgique, reçoit une carte à voter, mais celle-ci sert uniquement à autoriser l'émission d'un vote par l'électeur. Le vote n'est pas enregistré sur la carte utilisée par l'électeur, mais est stocké dans la mémoire de la machine. Lors de la clôture du bureau de vote, chaque machine à voter délivre, via une imprimante incorporée, un formulaire papier qui rend compte de ses résultats. En outre, chaque machine est dotée d'une carte mémoire détachable qui contient aussi une copie des votes émis sous forme cryptée. Cette carte est protégée contre le retrait par des personnes non autorisées au moyen d'une serrure.

Dans cette discussion, le point important concerne la manière dont le logiciel est mis à jour sur la machine. La mémoire interne de l'appareil à voter contient en effet, en plus des votes émis, le logiciel de vote lui-même. Pour installer une nouvelle version du logiciel, celle-ci est copiée sur la carte mémoire détachable, qui est insérée dans la machine, et la machine redémarre. Lors du démarrage de la machine, celle-ci vérifie si un logiciel est présent sur la carte détachable, et, si c'est le cas, ce dernier est installé, l'ancien logiciel étant écrasé.

5.1.2 L'attaque

Les chercheurs mentionnés précédemment ont réussi à écrire un nouveau logiciel frauduleux pour la machine à voter et à l'installer sur celle-ci. Ce logiciel se comporte, du point de vue de l'électeur et des membres du bureau de vote et de totalisation, exactement comme le vrai logiciel. La différence est toutefois que ce logiciel, pendant les opérations de vote, vole les voix d'un partie ou candidat au profit d'un autre parti ou candidat. Ceci est rendu possible, du fait que tous les votes déjà émis sont enregistrés dans la mémoire de la machine. Le fait que les résultats soient sauvegardés de manière cryptée tant dans la mémoire de la machine que sur la carte de mémoire détachable ne présente pas de problème digne d'être mentionné selon les chercheurs. Lorsque l'élection est clôturée, la liste imprimée et la carte de mémoire contiendront des données trafiquées. En outre, après la fin des élections, il est impossible de constater qu'un logiciel frauduleux a été utilisé. Lors de la clôture du bureau de vote, le logiciel frauduleux efface toute preuve de son passage et il n'est donc plus possible d'en retrouver la trace.

Le point crucial de l'attaque, une fois le logiciel frauduleux écrit, réside dans l'installation de ce logiciel sur les machines de vote. Il semble que la possibilité de mettre à jour le logiciel peut être facilement utilisée de manière détournée pour ce faire. La carte mémoire détachable uti-

gebruikt wordt door de stemmachine is een standaard computeronderdeel dat vrij in de handel te verkrijgen is. De software kan dus op deze kaart geplaatst worden, als het ware een update voor de software. Als deze kaart verwisseld wordt met de kaart aanwezig in de machine, en de machine wordt herstart, zal de frauduleuze software vanzelf geïnstalleerd worden. Om dit ongemerkt te kunnen doen schijnen er twee obstakels te zijn : ten eerste de geheugenkaart aanwezig in de machine is beveiligd door een slot, en ten tweede de machine maakt en luide pieptoon als hij herstart. Het eerste obstakel is gemakkelijk te verhelpen : het blijkt dat van de sleutels die gebruikt worden in de stemmachines er duizenden in omloop zijn (ze worden onder andere gebruikt voor minibars in hotels), dat ze vrij verkrijgbaar zijn in de handel en daarenboven makkelijk te kopiëren. Erger nog, zelfs zonder sleutel zijn de sloten gemakkelijk te openen, rapporteren de onderzoekers. Het tweede obstakel, de pieptoon is nog makkelijker te verhelpen : het aansluiten van een koptelefoon op de koptelefoonuitgang van de stemmachine deactiveert de luidspreker, net zoals in elke moderne draagbare computer. Eenmaal de software aldus geïnstalleerd, kan de verwijderbare geheugenkaart vervangen worden door de originele kaart, en is de verwijderbare kaart beschikbaar om een andere machine aan te vallen.

De hele procedure van het vervangen van de software door frauduleuze software duurt, volgens de onderzoekers, minder dan één minuut, en kan uitgevoerd worden door iedereen die toegang heeft tot de computers. Dit kan met andere woorden dus zelfs gebeuren op de dag van de verkiezingen zelf, en dit geheel ongemerkt.

Volgens de onderzoekers is het fundamenteel onderliggend probleem dat deze aanval mogelijk maakt de DRE techniek, en kan deze aanval gemakkelijk herhaald worden voor andere machines die dezelfde techniek gebruiken. Deze bewering wordt ondersteund door de recente evenementen in Nederland, die we verder in meer detail bespreken. De onderzoekers argumenteren verder dat de beste oplossing om dit soort aanvallen te vermijden een zogenaamde Voter-Verifiable Paper Trail (VVPAT) is, gecombineerd met willekeurige audits. Bij VVPAT wordt een papieren logboek aangemaakt, waar de stemmer zijn uitgebrachte stem kan zien. Dit kan bijvoorbeeld door zijn stem ook te printen op de magneetkaart die hij gebruikt.

Willekeurige audits worden dan uitgevoerd door een onafhankelijk organisme, waar de elektronische resultaten worden vergeleken met de papieren resultaten.

Meer gedetailleerde informatie, inclusief een video die de hele procedure toont is te vinden op de webstek van de universiteit van Princeton, centre of Information Technology Police, namelijk http://itpolicy.princeton.edu/voting.

lisée par la machine de vote est un composant d'ordinateur standard qui peut être obtenu librement dans le commerce. Le logiciel peut donc être installé sur cette carte, comme si c'était une mise à jour du logiciel. Si cette carte est échangée avec la carte présente dans la machine, et si celle-ci est redémarrée, le logiciel frauduleux s'installera de lui-même. Pour passer inaperçu, il y a deux obstacles à franchir : en premier lieu, la carte de mémoire présente dans la machine est protégée par une serrure, et en second lieu, la machine émet un bip très sonore quand elle redémarre. Le premier obstacle est facile à contourner : il apparaît que les clés utilisées dans les machines de vote sont très communes (elles sont utilisées entre autres pour les mini bars dans des hôtels), qu'elles sont disponibles dans le commerce et en plus faciles à copier. Et encore, même sans clé, les serrures sont faciles à ouvrir, rapportent les chercheurs. Le deuxième obstacle, le bip sonore, est encore plus facile à contourner : le raccordement d'un écouteur sur la sortie casque de la machine de voix désactive le haut-parleur, comme c'est le cas pour tout ordinateur portable moderne. Dès lors, une fois le logiciel installé, la carte d'origine « X » peut être remplacée par la carte originale, et la carte détachable d'origine « X » peut servir à attaquer une autre machine.

L'opération de remplacement du logiciel par le logiciel frauduleux demande, selon les chercheurs, moins d'une minute, et peut être effectuée par quiconque a accès aux ordinateurs. En d'autres termes, ceci peut donc même s'exécuter le jour des élections, et ceci entièrement de manière inaperçue.

Selon les chercheurs, le problème fondamental sous-jacent qui rend cette attaque possible, est la technique DRE, et cette attaque peut être reproduite facilement avec d'autres machines utilisant cette même technique. Cette affirmation est confirmée par les événements récents qui se sont déroulés aux Pays-Bas et sur lesquels nous revenons plus en détail dans la suite du rapport. Les chercheurs argumentent ensuite que la meilleure solution pour éviter ce type d'attaque est ce qu'on peut appeler un « Voter-Verifiable Paper Trail (VVPAT) » en combinaison avec des audits aléatoires. Dans le cas du « VVPAT », un journal papier est fabriqué, dans lequel l'électeur peut visualiser son vote. Ceci peut se réaliser par exemple, en imprimant son vote également sur la carte magnétique qu'il utilise.

Les audits aléatoires sont alors effectués par un organisme indépendant, où les résultats électroniques sont comparés avec les papiers résultats.

Une information plus détaillée, incluant une vidéo qui montre la procédure dans sa totalité est consultable sur le site Internet de l'université de Princeton, « center for Information Technology Policy », à l'adresse http://itpolicy.princeton.edu/voting.

5.1.3. Vergelijking met het Belgische systeem

De aanval op de stemcomputer zoals boven beschreven is gebaseerd op het feit dat de uitgebrachte stemmen in het geheugen van de stemcomputer zijn opgeslagen. In het Belgische systeem is dit niet het geval, hier worden de stemmen opgeslagen op de computer van de voorzitter, of in de urne, naargelang het gebruikte systeem (vanaf nu « de urne » genoemd). Om een analoge aanval uit te voeren moet dus deze machine het doelwit zijn.

De vraag is dus te herformuleren als : hoe kunnen we de software van urne vervangen door frauduleuze software. Dit ongemerkt laten doen door een stemmer is hier duidelijk uitgesloten, aangezien het herstarten van een urne niet onopgemerkt kan gebeuren. De overblijvende optie is bij het openen de urne opstarten met frauduleuze software. De procedure voor het opstarten van een stembureau, indien correct gevolgd, maakt dit echter zeer moeilijk. Dit gekoppeld aan de controles door het college van de gebruikte software in de urne, in willekeurige stembureaus, maakt de kans voor het onopgemerkt plaats vinden van deze vorm van fraude extreem klein.

5.2. Nederland

In Nederland is er op 4 oktober een discussie ontstaan, gelijkaardig aan die in de VS, over de stemmachines die gebruikt worden voor het uitbrengen van 90 % van de stemmen. Een onafhankelijke groep van experts, de stichting « wij vertrouwen stemcomputers niet » (vanaf nu genoemd « de stichting ») heeft een volledige analyse gemaakt van deze computer. De stichting is er ook in geslaagd een van deze computers, die in hun bezit is, te herprogrammeren zodanig dat deze fraudeert met stemmen, analoog aan het stelen van stemmen gedemonstreerd door de onderzoekers van Princeton.

5.2.1. De hardware

De machine in kwestie is een Nedap ES3B machine, en wordt gebruikt in het overgrote deel van de Nederlandse gemeentes. Deze machine werkt vrij analoog aan de Diebold machine hierboven beschreven. Een totaal van de uitgebrachte stemmen wordt opgeslagen op een verwijderbare geheugenmodule, die net zoals in de VS beveiligd is met een sleutel. Een eerste verschil is dat bij het sluiten van het stembureau deze module verwijderd wordt, en op een aparte machine uitgelezen wordt voor totalisatie. Een tweede verschil met het systeem in de VS is dat deze geheugenmodule geen software bevat. Hier is de software opgeslagen op 2 chips die zich intern in de machine bevinden.

5.1.3 La comparaison avec le système belge

L'attaque de la machine à voter décrite ci dessus est basée sur le fait que les votes émis sont enregistrés dans la mémoire de la machine de vote. Dans le système belge, ce n'est pas le cas : les votes y sont enregistrés sur l'ordinateur du président ou dans l'urne, selon le système utilisé (le terme « urne » est par la suite utilisé pour les 2 systèmes). Pour lancer une attaque analogue, c'est donc cette urne qui doit être la cible.

La question est donc à reformuler comme suit : comment peut-on remplacer le logiciel d'urne par un logiciel frauduleux ? Qu'un électeur puisse le faire sans que cela soit détecté est clairement exclu, étant donné que le redémarrage d'une urne ne peut pas passer inaperçu. L'alternative consiste à démarrer l'urne avec le logiciel frauduleux. La procédure pour le démarrage d'un bureau de vote, si elle est suivie correctement., rend toutefois ceci très difficile. La procédure à laquelle s'ajoutent les contrôles du logiciel utilisé dans l'urne, contrôles réalisés par le collège des experts dans des bureaux choisis au hasard, rend extrêmement improbable la réalisation dissimulée de cette forme de fraude.

5.2. Pays-Bas

Le 4 octobre une discussion similaire à celle ayant eu lieu aux Etats-Unis a surgi au sujet des machines à voter qui sont utilisées pour émettre 90 % des voix. Un groupe indépendant d'experts, la fondation « wij vertrouwen stemcomputers niet » (littéralement « nous n'avons pas confiance dans les ordinateurs à voter » – à partir de maintenant nous parlerons de « de stichting ») a procédé à une analyse de cet ordinateur. « De stichting » qui possède un de ces ordinateurs a réussi à reprogrammer celui-ci de telle façon qu'il fraude au niveau des voix, d'une façon similaire au vol de voix programmé par les chercheurs de Princeton.

5.2.1. Le matériel

La machine en question est un Nedap ES3B et est utilisée dans la majorité des communes néerlandaises. Cette machine fonctionne de façon assez analogue à la machine Diebold décrite ci-dessus. Le total des voix émises est sauvegardé sur un module de mémoire détachable qui est protégé tout comme aux Etats-Unis avec une clé. Une première différence est que lors de la fermeture du bureau de vote, ce module est retiré, et est relu sur une machine séparée pour la totalisation. Une deuxième différence avec le système aux Etats-Unis est que le module de mémoire ne contient pas le logiciel. Dans le cas de Pays-Bas le logiciel est stocké sur deux puces qui se trouvent dans la machine.

5.2.2. De aanval

Het eerste gedeelte van de aanval concentreert zich op het gebruik van sleutels. De Nederlandse wet vereist onder andere de aanwezigheid van een sleutel in de stemmachine om te kunnen stemmen, maar stelt geen vereisten aan de kwaliteit van de sloten. De stichting stelt dat alle stemmachines in Nederland bediend kunnen worden met slechts 1 sleutel, en daarenboven dat deze sleutel vrij verkrijgbaar is voor de prijs van 1 EUR. Ten gevolge hiervan beschouwen ze deze beveiliging als waardeloos, wat leid tot een situatie analoog aan de boven beschreven situatie in de VS.

Het tweede gedeelte van de aanval bestaat er in van de stemsoftware te vervangen door frauduleuze software. Hoewel de software opgeslagen is intern in de computer, blijkt het zeer eenvoudig te zijn om deze twee chips te vervangen door andere, die frauduleuze software bevatten. Deze chips zijn standaard computeronderdelen en zijn vrij in de handel te verkrijgen. Volgens de stichting vereist deze operatie enkel een schroevendraaier en neemt ze minder dan 5 minuten in beslag. Als bewijs dat het mogelijk is om op deze manier te frauderen heeft de stichting zelf frauduleuze software geschreven, genaamd Nedap PowerFraud. Net zoals de software geschreven door de onderzoekers in de VS, steelt deze software ongemerkt stemmen.

De enige manier om te kunnen ontdekken of er gefraudeerd is bij deze machines is om na de verkiezingen de machines te demonteren en de programmachips te onderzoeken. Als deze andere software bevatten dan de officiële software, is er indicatie van fraude.

Meer gedetailleerde informatie, met verwijzingen naar Tv-reportages die hierover rapporteren is te vinden op de webstek van de stichting namelijk http://www.wijvertrouwenstemcomputersniet.nl.

5.2.3. Vergelijking met het Belgische systeem

Aangezien de aanval analoog is aan de aanval uitgevoerd op de stemmachines in de VS, is de vergelijking met het Belgische systeem analoog. De software van de urne moet vervangen worden door frauduleuze software. Dit heeft in België, als de procedures correct gevolgd worden, in combinatie met controles door het college, een extreem lage waarschijnlijkheid om onopgemerkt te kunnen gebeuren.

6. Aanbevelingen

6.1. Rol van het MBHG in de organisatie

De overheden belast met de organisatie van de verkiezingen zouden de kwaliteit en de doeltreffendheid van de broncode in een audit moeten laten onderzoeken. Daarom zou de software enkele maanden voor de dag van de verkiezingen klaar moeten zijn.

5.2.2. L'attaque

Le première partie de l'attaque se concentre sur l'utilisation des clés. La loi néerlandaise exige entre autres la présence d'une clé dans la machine à voter afin de pouvoir voter, mais n'a pas d'exigences concernant la qualité de la serrure. « De stichting » affirme que toutes les machines à voter aux Pays-Bas peuvent être desservies avec une même clé, et en outre que cette clé se trouve facilement dans le commerce et ne coûte que 1 EUR. Ce qui leur fait conclure que cette protection est sans valeur, ce qui mène à une situation analogue à celle aux Etats-Unis.

La deuxième partie de l'attaque consiste à remplacer le logiciel de machine à voter par un logiciel frauduleux. Bien que le logiciel soit stocké à l'intérieur de l'ordinateur, il apparaît qu'il est très simple de remplacer ces deux puces par d'autres sur lequel se trouve le logiciel frauduleux. Ces puces sont des parties standard d'ordinateur et se trouvent librement dans le commerce. Selon « de stichting » cette opération ne demande qu'un tournevis et prend moins de 5 minutes. « De stichting » a elle-même écrit un logiciel frauduleux afin de prouver qu'il est possible de frauder. Ce logiciel est appelé Nedap PowerFraud. Tout comme le logiciel écrit par les chercheurs aux Etats-Unis, ce logiciel vole des voix de façon imperceptible.

L'unique façon de découvrir qu'il a été fraudé lors de l'élection est démonter ces machines après les élections et d'analyser les puces contentant les logiciels. Si celles-ci contiennent un autre logiciel que le logiciel officiel, il y a indication de fraude.

Des informations plus détaillées, avec des liens vers des reportages télévisuels en rapport avec ce sujet se trouvent sur le site web de « De stichting » : http://www.wijvertrouwenstemcomputersniet.nl.

5.2.3. La comparaison avec le système belge

Étant donné que l'attaque est analogue à l'attaque sur les machines à voter des Etats-Unis, la comparaison avec le système belge est également analogue. Le logiciel de l'urne doit être remplacé par un logiciel frauduleux. Les contrôles effectués par le collège ainsi que les procédures – si elles sont suivies correctement – rendent l'éventualité d'une fraude peu probable.

6. Recommandations

6.1. Rôle du MRBC dans l'organisation

Les autorités en charge des élections devraient faire procéder à un audit sur la qualité et la pertinence du code source des logiciels des élections. Pour ce faire, le code définitif des logiciels devrait être finalisé plusieurs mois avant le jour des élections.

De autoriteiten zouden eveneens alle procedures bij het voorbereiden van de verkiezingen, de verkiezingen zelf en de totalisatie in een audit moeten laten evalueren.

Er zou een analyse moeten uitgevoerd worden over de manier om best « random » getallen te genereren bestemd voor de aanmaak van encryptie sleutels en initiële waarden.

Er zou meer zorg moeten worden gedragen bij het opstellen van het handboek voor de voorzitters. Deze zou minstens twee maanden voor de verkiezingen beëindigd moeten worden zo dat alle voorzitters over dezelfde informatie beschikken.

Daarnaast moeten de gemeentes de officiële procedures naleven en ervoor zorgen dat die worden gevolgd.

6.2. Algemene veiligheid

De vier lettertekens die op unieke wijze verbonden zijn aan de de aan de gang zijnde verkiezingen mogen op geen enkele evidente wijze deel uitmaken van de broncode van de software van de kiesverrichtingen.

Een veiligheidspolitiek dient opgesteld te worden om ondermeer maatregelen te nemen ten einde de software en digitale opslagmiddelen te beschermen tegen programmatuur van slechte wil. Een dergelijke veiligheidspolitiek moet ook de regels omvatten voor het ontwerpen van software, het versturen van zowel software als gegevens, de vertaling van de broncode naar machinecode, de aanmaak van de diskettes en het versturen ervan.

Het verpakken van de diskettes in een omslag (ter bestemming van de voorzitters van de kiesbureaus) dient gepaard te gaan met een verzegeling van deze omslagen op een gewaarborgd veilige manier (een gebroken zegel mag niet op eenvoudige wijze kunnen worden hersteld, vervangen of vervalst). De procedures moeten voorzien dat de leden van een kiesbureau controleren en getuigen dat de omslag die de diskettes bevat en die aan de voorzitter van het kiesbureau overhandigd werd, wel degelijk verzegeld was op het ogenblik van de opening van het kiesbureau.

Om de veiligheid te versterken zou het opportuun zijn om het wachtwoord van de diskettes te scheiden tot het moment van de start van de stemlokalen.

6.3. Veiligheid in de stembureaus

Het moet verboden zijn om een computer binnen te brengen in het kiesbureau, met uitzondering van de computers eigen aan het kiesbureau (en van de machines die nodig zouden zijn voor de helpdesktechnici en voor de deskundigen belast met de controle van de geautomatiseerde stemming).

Les autorités devraient également faire procéder à un audit de toutes les procédures intervenant dans la préparation des élections et dans les opérations de vote et de totalisation.

Une analyse quant à la manière de générer les nombres aléatoires nécessaires à la création des clés cryptographiques et des valeurs initiales devrait être réalisée.

Un plus grand soin devrait être apporté à la rédaction du manuel des présidents de bureau de vote. Celui-ci devrait être terminé au moins deux mois avant les élections de façon à ce que tous les présidents disposent des mêmes informations.

De plus, les communes doivent veiller à respecter et à faire respecter les procédures officielles.

6.2. Sécurité globale

Les quatre caractères associés univoquement à une élection ne devraient pas faire partie tels quels des sources des logiciels des élections.

Une politique de sécurité décrivant, entre autres, l'ensemble des mesures mises en place pour protéger les logiciels et les supports utilisés contre des programmes malveillants devrait être rédigée. Une telle politique de sécurité détaillerait aussi les règles imposées quant à la conception des logiciels, la transmission des logiciels, la transmission des données, la compilation des logiciels, la création des disquettes et la transmission de ces disquettes.

Lors de la mise sous enveloppe des disquettes (à destination finale des présidents de bureaux de vote), ces enveloppes devraient être scellées d'une manière sécurisée (un sceau brisé ne pouvant être reconstitué, remplacé ou falsifié aisément). Les procédures devraient prévoir que tous les membres d'un bureau de vote vérifient et attestent, au moyen d'un document à signer, que l'enveloppe contenant les disquettes reçue par le président du bureau est bien toujours scellée à la constitution du bureau de vote.

Pour renforcer la sécurité, il serait opportun de séparer le mot de passe des disquettes jusqu'au moment du démarrage des bureaux de vote.

6.3. Sécurité dans les bureau de vote

En dehors des ordinateurs nécessaires aux procédures de votes, l'introduction dans un bureau de vote d'un ordinateur tiers devrait être interdite (à l'exception des ordinateurs qui seraient nécessaires aux techniciens du helpdesk ou de ceux des expertes chargés du contrôle du vote automatisé).

De diskettelezers, alsook de contacten aan de achterzijde van de verschillende machines, mogen niet toegankelijk zijn voor de kiezers.

Het is nodig om eraan te herinneren dat de fysieke veiligheid van de machines belangrijk is om de goede werking van de verrichtingen van dag van de verkiezingen te garanderen. Het college heeft vastgesteld dat dit punt in bepaalde gemeentes werd verwaarloosd en dat dit aspect zou moeten verbeterd worden.

6.4. Werking van de systemen en de broncode

De broncode dient publiek gemaakt te worden voor de dag van de verkiezingen.

In een volgende versie van de geautomatiseerde stemming zou het wenselijk zijn de kiezer de zekerheid te geven over de overeenkomst tussen de uitgebrachte stem en de inhoud van de magneetkaart. De gebruikte drager (magneetkaart of andere) voor de geautomatiseerde stemming zou moeten toelaten de stem zowel elektronisch als rechtstreeks leesbaar voor de kiezer op te nemen (bijvoorbeeld afgedrukt in tekstvorm op de kaart).

Men heeft vastgesteld dat de duur van invoering van een kaart in de Digivote stembussen 8 seconden kan duren. Dit zou sneller moeten kunnen.

Het is tevens te vermijden dat noch de software, noch het paswoord te vroeg in de handen van de voorzitter van het kiesbureau terechtkomen.

Overigens suggereert het college met betrekking tot het schrijven van de software :

– Om alle wisprocedures van magnetische media fysiek uit te voeren : alle informatie dient effectief overschreven te worden.

– Om te waken over de robuustheid van de encryptering van de individuele stemmen.

– Om correcte methodologische regels van goed gebruik op te leggen tijdens het ontwerp en verwezenlijking van de software.

7. Besluiten

Binnen de grenzen van de opdracht, de middelen en de beschikbare tijd, besluit het college het volgende.

Op basis van het in de tijd beperkte nazicht van de programmatuur, de uitgevoerde testen, steekproeven en controles na de stemming, heeft het college geen technische disfuncties in de stemsystemen, fouten of fraudepogingen

Tout comme les lecteurs de disquettes, les connecteurs, qui se trouvent à l'arrière des différentes machines, devraient être rendus physiquement inaccessibles.

Il convient de rappeler que la sécurité physique des machines revêt une importance réelle pour garantir le bon fonctionnement des opérations le jour des élections. Les constatations du collège dans certaines communes montrent que cet aspect est négligé et devrait être amélioré.

6.4. Fonctionnement des systèmes et codes source

Les sources des logiciels des élections devraient être publiées avant le jour des élections.

Dans une prochaine mouture du vote automatisé, il serait souhaitable de donner plus de garantie à l'électeur quant à la correspondance entre le vote qu'il a émis et le contenu de la carte magnétique. Le support utilisé (carte magnétique ou autre) pour le vote automatisé devrait donc permettre d'enregistrer le vote tant de manière informatique que directement visible pour l'électeur (par exemple impression sous forme de texte sur la carte).

Il a été constaté que la durée d'introduction d'une carte dans les urnes Digivote peut atteindre 8 secondes, ce qui devrait être amélioré.

Il est aussi nécessaire de ne pas concentrer dans les mains des présidents de bureaux de vote, trop longtemps avant les élections, à la fois leur mot de passe et les logiciels des élections.

Par ailleurs, quant à l'écriture des programmes, le collège suggère :

– De manière générale, de procéder à la destruction physique des fichiers effacés : toutes les informations doivent être effectivement écrasées.

– De s'assurer de la robustesse de la méthode de chiffrement des votes individuels.

– D'imposer des règles méthodologiques et de bonnes pratiques pour l'écriture et la conception du code des logiciels.

7. Conclusions

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

Sur la base de la vérification des logiciels limitée par le temps, des tests et simulations effectuées, des tests par échantillonnage et des contrôles effectués après le vote, le collègue n'a pas constaté de dysfonctionnement au niveau

vastgesteld die het gebruik en de goede werking ervan tijdens de provincie- en gemeenteraadsverkiezingen van 8 oktober 2006 belemmerden.

De onafhankelijke totalisatie door het college bevestigt dat de totalisatie van alle diskette afkomstig uit de stembureaus geen fouten opleverde.

Het beoogde doel, namelijk het uitbrengen, opslaan, weergeven en tellen van de stemmen overeenkomstig de wetsbepalingen, werd bereikt.

Het college benadrukt dat het respecteren van de procedures een optimale veiligheid garandeert. Parallelle of laattijdig verspreidde onderrichtingen bieden een gunstige voedingsbodem voor incidenten.

Het college beveelt ook aan dat de relatie tussen het adviesorgaan en de leveranciers van de software van het automatisch stemsysteem wordt herzien zodat de onafhankelijke positie van het adviesorgaan kan worden versterkt.

Het college zal, vanaf de publicatie van de broncode, een vervolg op dit verslag overhandigen met daarin de resultaten van de analyse van de overeenstemming tussen die broncode en de broncode gebruikt bij de referentiecompilatie.

Het college wenst ten slotte de medewerkers van de MBHG, de vertegenwoordigers van de firma's en van het adviesorgaan, de voorzitters, bijzitters en getuigen in de stem- en totalisatiebureaus en de gemeentelijke verantwoordelijken te danken voor de goede en bereidwillige samenwerking.

Jean-Marc Paul
Voorzitter

Sophie Jonckheere
Secretaris

Geert Bryon | Freddy Tomicki | Theo D'Hondt

Emmanuel Willems | Johan Fabry | Olivier Markowitch

technique dans les systèmes de vote, d'erreurs ou de tentatives de fraude susceptibles d'entraver l'utilisation et le bon fonctionnement des systèmes de votes lors des élections du 8 octobre 2006.

La totalisation indépendante à laquelle le collège s'est livrée permet par ailleurs d'affirmer que la totalisation à partir des disquettes en provenance des bureaux de vote n'a engendré aucune erreur.

L'objectif visé, à savoir émettre les votes, les enregistrer et les compter selon les dispositions légales, a été atteint.

Le collège tient à insister sur l'importance du respect des procédures, garantie d'une sécurité optimale. Des instructions parallèles ou tardivement transmises ne peuvent que créer un terrain propice aux incidents.

Par ailleurs, le collège recommande que les relations entre l'organisme d'avis et le fournisseur du logiciel des systèmes de vote automatisé soient revues de façon à renforcer la position d'indépendance de l'organisme d'avis.

Le collège s'engage, dès la publication du code source, à remettre un avenant au présent rapport, reprenant les résultats de l'analyse de la conformité du code source publié avec celui utilisé lors de la compilation de référence.

Enfin, le collège remercie les fonctionnaires du MRBC, les représentants des firmes et de l'organisme d'avis, les présidents, assesseurs et témoins des bureaux de vote et de totalisation ainsi que les responsables communaux pour leur bonne collaboration et pour leur coopération.

Jean-Marc Paul
Président

Sophie Jonckheere
Secrétaire

Geert Bryon | Freddy Tomicki | Theo D'Hondt

Emmanuel Willems | Johan Fabry | Olivier Markowitch

1006/8151
I.P.M. COLOR PRINTING
☎ 02/218.68.00