



Rapport du Collège d'experts
chargés du contrôle du système
de vote et de dépouillement
automatisés

Version provisoire

Les élections simultanées du
25 mai 2014

le 9 juin 2014

Verslag van het College van
deskundigen belast met de
controle van het elektronisch
stem- en
stemopnemingssysteem

Voorlopige versie

Gelijktijdige verkiezingen van
25 mei 2014

9 juni 2014

Table des Matières - Inhoudstafel

1	Avertissement – Woord vooraf.....	6
2	Composition du Collège – Samenstelling van het College	6
2.1	Collège permanent - Het permanent College.....	6
2.2	Le Collège non permanent - Het niet-permanent College.....	7
2.3	Composition du Collège d'experts lors des élections simultanées du 25 mai 2014 Samenstelling van het College van Deskundigen bij de gelijktijdige verkiezingen van 25 mei 2014.....	7
2.4	La mission du Collège lors des élections du 25 mai 2014 De opdracht van het College bij de verkiezingen van 25 mei 2014.....	8
2.4.1	Cadre légal - Wettelijk kader.....	8
2.4.2	La nature de la mission : collecte d'informations et contrôle De aard van de opdracht: informatieverzameling en controle	9
3	Description des systèmes de vote automatisé.....	10
3.1	Le vote automatisé sans preuve papier (Jites / Digivote)	10
3.2	Le vote automatisé avec preuve papier (SmartMatic).....	11
3.2.1	Les systèmes	11
3.2.2	La procédure électorale avec preuve papier	12
3.3	Le système CODI	13
3.4	Le système DePass – E-counting	13
3.5	Le système Web2	13
4	Contrôles et constatations.....	13
4.1	Contrôles effectués avant le jour des élections	13
4.1.1	La certification des logiciels électoraux	16
4.1.2	Le système SmartMatic.....	16
4.1.3	Le système Jites.....	16
4.1.4	Le système CODI	17
4.1.5	Confection des supports mémoires – Vervaardiging van de geheugendragers	17
4.1.6	Participation aux séances de formations des présidents de bureaux de vote	17
4.1.7	Authenticité des codes sources	18
4.1.8	Analyse des codes sources	18
4.1.9	Sécurité des systèmes.....	19
4.2	Constatations le jour des élections	19
4.2.1	Contrôles dans les bureaux de votes	21
4.2.2	Contrôle dans les bureaux de dépouillement (DEPASS - E-Counting)	21
4.2.3	Contrôle du système Web2.....	22
4.2.4	Contrôles dans les bureaux de totalisation.....	22
4.3	Contrôles effectués après le jour des élections.....	22
4.3.1	Vérification des votes de référence	22
4.3.2	Vérification des totalisations	25
4.3.3	Diffusion des codes source	25
4.3.4	Suivi des recommandations des rapports précédents.....	25
5	Chronologie du "bug des élections 2014".....	25
5.1	Détection du bug : blocage des totalisatrices – 25 mai.....	26
5.1.1	Constat	26
5.1.2	Conséquence.....	26
5.1.3	Première explication du blocage.....	27
5.1.4	Déblocage des totalisatrices	27
5.2	Explication du bug – 26 mai.....	27

5.3	Premier calcul de l'impact du bug – 26 mai et 27 mai	28
5.3.1	Développement de deux programmes <i>ad hoc</i>	28
5.3.2	Calcul des votes invalides.....	28
5.3.3	Impact sur la répartition des sièges entre les listes et entre les candidats d'une même liste après annulation des votes invalides	28
5.3.4	Impact sur la répartition des sièges entre les listes après annulation des votes invalides et report de ces votes selon un scénario « pire des cas ».....	29
5.3.5	Impact sur la répartition des sièges entre candidats d'une même liste selon un scénario « pire des cas »	29
5.4	Corrections proposées aux bureaux principaux des circonscriptions électorales – 27 mai.....	29
5.5	Corrections apportées au niveau des circonscriptions électorales – du 28 mai au 30 mai.....	30
5.6	Rapport de la firme Stésud au Collège d'experts – 30 mai.....	30
5.6.1	Les tableaux de corrections pour Bruxelles étaient incorrects.....	30
5.6.2	Le décryptage des urnes électroniques était incorrect	31
5.6.3	Des urnes électroniques étaient toujours manquantes	31
5.7	Contrôles du Collège - du 31 mai au 1 ^{er} juin	31
5.7.1	Logiciel de décryptage développé par le Collège.....	31
5.7.2	Logiciel d'identification et de totalisation des votes invalides	31
5.7.3	Méthode GREP	31
5.8	Suite des corrections – du 2 au 5 juin	32
5.8.1	Communication au SPF Intérieur et à Stésud	32
5.8.2	Identification des urnes manquantes ou incorrectes	32
5.8.3	Récolte des urnes manquantes.....	32
5.8.4	Décompte des votes invalides	32
5.9	Calcul final de l'impact des votes invalides sur la répartition des sièges entre les listes – 5 juin	33
5.10	Analyse du code source ayant généré le « Bug de l'élection 2014 »	33
5.10.1	Stockage des votes en mémoire	33
5.10.2	Sélection d'un candidat	33
5.10.3	Désélection d'un candidat	34
5.10.4	Ecriture sur la carte magnétique	34
5.10.5	Identification des votes invalides	35
5.11	Considérations générales sur le « Bug »	35
5.12	Informations chiffrées du « bug des élections 2014 »	36
5.12.1	Identification des votes invalides par la méthode GREP	36
5.12.2	Identification par des votes individuels par circonscription, canton, élection et liste.....	36
6	Recommandations	37
6.1	A propos du système SmartMatic	37
6.2	A propos du système Jites	37
6.3	A propos du système CODI	37
6.4	A propos du bon usage de la cryptographie	37
6.5	À propos de la gestion des mots de passe	38
6.6	À propos de l'expression des votes.....	38
6.7	A propos du matériel	39
6.8	A propos du développement des logiciels des élections	39
6.9	A propos de la documentation des logiciels des élections.....	39
6.10	A propos du respect des procédures.....	39
6.11	Liste non-exhaustive de recommandations issues des rapports précédents du Collège non-respectées durant les élections 2014	40
7	Conclusions – Besluiten	42
8	Annexes	48

8.1	Tableaux de calcul du « bug des élections 2014 »	48
8.1.1	Circonscription de Bruxelles-capitale.....	48
8.1.2	Province de Liège (à l'exception des cantons germanophones)	60
8.1.3	Cantons germanophones.....	71
8.1.4	Province du Hainaut.....	73
8.1.5	Province du Luxembourg - Canton de Durbuy.....	75
8.2	Formations	76
8.3	Contrôles des bureaux de vote	78
8.4	Contrôles des bureaux de totalisation	79

Woord vooraf

Bij gebrek aan tijd en middelen heeft het College niet kunnen overgaan tot het vertalen van dit verslag. De huidige versie is een voorlopige gemengde Franse-Nederlandse tekst. Het College zal in de komende dagen overgaan tot de vertaling van zijn verslag en zal een volledige definitieve tweetalige versie aan de assemblees en aan de Minister van Binnenlandse Zaken bezorgen.

Préambule

Par manque de temps et de moyens, le Collège n'a pas pu procéder à la traduction du présent rapport. La présente version est une version provisoire panachée français-néerlandais. Le Collège procédera à la traduction de son rapport dans les prochains jours et fournira aux assemblées et à la Ministre de l'Intérieur une version définitive bilingue complète.

1 Avertissement – Woord vooraf

Étant donné la nature de la mission du Collège, le présent rapport est par endroit assez technique et s'adresse donc à un public averti. Néanmoins, le Collège a essayé lorsque c'était possible de vulgariser ces propos tout en veillant à rester précis.

Gelet op de aard van de opdracht van het College, is dit rapport zonder meer vrij technisch en dus bedoeld voor een publiek met kennis van zaken. Niettemin heeft het College geprobeerd om, indien mogelijk, het woordgebruik begrijpelijk te houden en tegelijk nauwkeurig te blijven.

2 Composition du Collège – Samenstelling van het College

2.1 Collège permanent - Het permanent College

Conformément aux articles 24 et 35 de la loi du 7 février 2014 organisant le vote électronique avec preuve papier (ci-après : loi du 7 février 2014), les experts suivants ont été désignés en vue de constituer le Collège permanent pour une durée de cinq ans :

1. Experts désignés par la Chambre des représentants :

- effectifs : M. Bruno DE NYS, M. Karel VAN GEYT et M. Emmanuel WILLEMS ;
- suppléants : Mme Sophie JONCKHEERE, M. Freddy TOMICKI et M. Erwin VEREECKEN.

2. Experts désignés par le Parlement flamand :

- effectif : M. Kurt DE VRIENDT ;
- suppléant : M. Romain VOES.

3. Experts désignés par le Parlement de la Région de Bruxelles-Capitale :

- effectif : M. Jean-Marc PAUL ;
- suppléant : M. Pascal VAN de WALLE.

4. Experts désignés par le Parlement de la Communauté germanophone :

- effectif : M. Daniel BRANDT ;
- suppléante : Mme Susi OSTLENDER.

Ces experts constituent le Collège d'experts permanent.

Le Parlement wallon n'a désigné aucun expert pour ce Collège permanent.

Conformément à l'article 24, § 2, alinéa 3, de la loi du 7 février 2014, les experts effectifs ont désigné en leur sein un président, M. Emmanuel WILLEMS, et un secrétaire, M. Jean-Marc PAUL.

Op grond van de artikelen 24 en 35 van de wet van 7 februari 2014 tot organisatie van de elektronische stemming met papieren bewijsstuk (verder: de wet van 7 februari 2014), werden de volgende deskundigen aangewezen om voor een periode van vijf jaar het permanent College te vormen:

1. Deskundigen aangewezen door de Kamer van volksvertegenwoordigers:

- effectief: de heer Bruno DE NYS, de heer Karel VAN GEYT en de heer Emmanuel WILLEMS;
- plaatsvervangend: Mevr. Sophie JONCKHEERE, de heer Freddy TOMICKI en de heer Erwin VEREECKEN.

2. Deskundigen aangewezen door het Vlaams Parlement:

- effectief: de heer Kurt DE VRIENDT;
- plaatsvervangend: de heer Romain VOES.

3. Deskundigen aangewezen door het Brussels Hoofdstedelijk Parlement:

- effectief: de heer Jean-Marc PAUL;
- plaatsvervangend: de heer Pascal VAN de WALLE.

4. Deskundigen aangewezen door het Parlement van de Duitstalige Gemeenschap:

- effectief: de heer Daniel BRANDT;
- plaatsvervangend: Mevr. Susi OSTLENDER.

Deze deskundigen vormen het permanent College van deskundigen.

Het Waals Parlement heeft geen deskundigen aangewezen voor dit permanent College.

Overeenkomstig artikel 24, § 2, derde lid, van de wet van 7 februari 2014, hebben de effectieve deskundigen in hun midden als voorzitter de heer Emmanuel WILLEMS en als secretaris de heer Jean-Marc PAUL aangewezen.

2.2 Le Collège non permanent - Het niet-permanent College

Conformément aux articles 24 et 35 de la loi du 7 février 2014 organisant le vote électronique avec preuve papier, les experts suivants ont été désignés en vue de constituer le Collège non permanent à l'occasion des élections simultanées du 25 mai 2014 pour le Parlement européen, la Chambre des représentants et les parlements de communauté et de région :

1. Experts désignés par la Chambre des représentants:

- M. Ralph RAIGLOT et M. Eric ADAMS.

2. Experts désignés par le Parlement wallon :

- M. Jean-François DAMSEAUX et Mme Véronique NACHTERGAELE.

3. Experts désignés par le Parlement flamand :

- M. Romeo MARYNS et M. Steven ES.

4. Experts désignés par le Parlement de la Région de Bruxelles-Capitale :

- M. Jérôme DOSSOGNE et M. Olivier MARKOWITCH.

5. Experts désignés par le Parlement de la Communauté germanophone :

- M. Bruno HICK et M. Manfred FETTWEIS.

Ces experts constituent le Collège d'experts non permanent.

Op grond van de artikelen 24 en 35 van de wet van 7 februari 2014 tot organisatie van de elektronische stemming met papieren bewijsstuk, werden de volgende deskundigen aangewezen om het niet-permanent College te vormen ter gelegenheid van de gelijktijdige verkiezingen van 25 mei 2014 voor het Europees Parlement, de Kamer van volksvertegenwoordigers en de Gewest- en Gemeenschapsparlamenten:

1. Deskundigen aangewezen door de Kamer van volksvertegenwoordigers:

- de heer Ralph RAIGLOT en de heer Eric ADAMS.

2. Deskundigen aangewezen door het Waals Parlement:

- de heer Jean-François DAMSEAUX en Mevr. Véronique NACHTERGAELE.

3. Deskundigen aangewezen door het Vlaams Parlement:

- de heer Romeo MARYNS en de heer Steven ES.

4. Deskundigen aangewezen door het Brussels Hoofdstedelijk Parlement:

- de heer Jérôme DOSSOGNE en de heer Olivier MARKOWITCH.

5. Deskundigen aangewezen door het Parlement van de Duitstalige Gemeenschap:

- de heer Bruno HICK en de heer Manfred FETTWEIS.

Deze deskundigen vormen het niet-permanent College van deskundigen.

2.3 Composition du Collège d'experts lors des élections simultanées du 25 mai 2014

Samenstelling van het College van Deskundigen bij de gelijktijdige verkiezingen van 25 mei 2014

Ensemble, le Collège permanent et le Collège non permanent constituent le Collège d'experts pour les élections simultanées du 25 mai 2014 pour le Parlement européen, la Chambre des représentants et les parlements de Communauté et de Région (ci-après le Collège).

Conformément à l'article 24, § 2, alinéa 4, de la loi du 7 février 2014, les experts suppléants désignés sont membres de plein droit du Collège d'experts pour les élections simultanées du 25 mai 2014.

En principe, le Collège travaille à partir du quarantième jour précédant l'élection, le jour de l'élection et après celle-ci, jusqu'au dépôt du rapport

Het permanent College en het niet-permanent College vormen samen het College van Deskundigen voor de gelijktijdige verkiezingen van 25 mei 2014 voor het Europees Parlement, de Kamer van volksvertegenwoordigers en de Gewest- en Gemeenschapsparlamenten (verder: het College).

Overeenkomstig artikel 24, § 2, vierde lid, van de wet van 7 februari 2014, zijn de aangewezen plaatsvervangende deskundigen leden van rechtswege van het College bij de gelijktijdige verkiezingen van 25 mei 2014.

Het College is in beginsel werkzaam vanaf de veertigste dag voor de verkiezing, op de verkiezingsdag zelf, en hierna tot de indiening van

(article 25, § 1er, alinéa 5, de la loi du 7 février 2014). Dès lors que la Chambre des représentants n'a désigné des experts qu'en date du 24 avril 2014, le Collège n'a pu exercer sa mission dans sa composition définitive qu'à partir de cette date.

het verslag (artikel 25, § 1, vijfde lid, van de wet van 7 februari 2014). Doordat de Kamer van volksvertegenwoordigers pas deskundigen heeft aangewezen op 24 april 2014, heeft het College zijn opdracht echter pas vanaf die datum in de definitieve samenstelling kunnen uitoefenen.

2.4 La mission du Collège lors des élections du 25 mai 2014 De opdracht van het College bij de verkiezingen van 25 mei 2014

2.4.1 Cadre légal - Wettelijk kader

La mission du Collège lors des élections du 25 mai 2014 découle de l'article 25, §§ 1er et 2, de la loi du 7 février 2014 :

« Art. 25. § 1er. Lors de l'élection des membres de la Chambre des représentants, du Parlement européen et des Parlements de communauté et de région, ces experts contrôlent la préparation, l'utilisation et le bon fonctionnement de l'ensemble de systèmes de vote, de décryptage, d'enregistrement et de totalisation électroniques ainsi que les procédures concernant la confection, la distribution et l'utilisation des appareils, des logiciels et des supports d'information électroniques. Le Collège d'Experts contrôle également la préparation, l'utilisation et le bon fonctionnement des matériels, logiciels et procédures de transmission et de diffusion digitale des résultats.

Les experts reçoivent du ministre de l'Intérieur ou de son délégué le matériel ainsi que l'ensemble des données, renseignements et informations utiles pour exercer un contrôle sur les systèmes de vote, d'enregistrement et de totalisation électroniques et sur les systèmes de transmission digitale des résultats. Les membres de bureaux électoraux, les organismes d'avis visés à l'article 4, § 3, alinéa 2, et les entreprises privées — ainsi que leurs membres — associées par les autorités compétentes au déroulement du processus électoral fournissent également aux experts le matériel ainsi que l'ensemble des données, renseignements et informations utiles pour exercer le contrôle visé à l'alinéa 1er.

Les experts peuvent notamment émettre dans les bureaux de vote — durant l'élection — des votes qui ne sont ni scannés ni comptabilisés, vérifier la fiabilité des logiciels des systèmes de vote, la transcription exacte des votes émis sur les bulletins de vote, la transcription exacte, par la lecture du code-barres présent sur chaque bulletin de vote, des suffrages exprimés sur le support de mémoire du bureau de vote, l'enregistrement exact du support de

De opdracht van het College bij de verkiezingen van 25 mei 2014 volgt uit artikel 25, § 1 en 2, van de wet van 7 februari 2014:

“Art. 25. § 1. Bij de verkiezing van de leden van de Kamer van volksvertegenwoordigers, van het Europees Parlement en de Gewesten Gemeenschapsparlamenten, zien deze deskundigen toe op de voorbereiding, het gebruik en de goede werking van alle elektronische stelsystemen, registratiesystemen, ontsleutelingssystemen en totaliseringssystemen, alsook de procedures betreffende de aanmaak, de verspreiding en het gebruik van de apparatuur, programmatuur en de elektronische gegevensdragers. Het College van Deskundigen controleert eveneens de voorbereiding, het gebruik en de goede werking van de hardware, software en procedures voor de digitale transmissie en het digitaal verspreiden van de resultaten.

De deskundigen ontvangen van de minister van Binnenlandse Zaken of zijn afgevaardigde het materiaal alsook alle gegevens, inlichtingen en informatie die nuttig zijn om een controle uit te voeren op de elektronische stelsystemen, de registratiesystemen en de totaliseringssystemen en op de systemen van digitale doorzending van de resultaten. De leden van de kiesbureaus, de in artikel 4, § 3, tweede lid, bedoelde adviesorganen en de privébedrijven — alsook hun leden — die door de bevoegde overheden betrokken zijn bij het verloop van het kiesproces leveren eveneens aan de deskundigen het materiaal alsook alle gegevens, inlichtingen en informatie die nodig zijn om de in het eerste lid bedoelde controle uit te voeren.

De deskundigen kunnen in het bijzonder — tijdens de verkiezing — stemmen uitbrengen die gescand noch geteld worden, de betrouwbaarheid controleren van de software in de stelsystemen, alsook de correcte overschrijving van de uitgebrachte stemmen op de stembiljetten, de correcte overschrijving, door het lezen van de barcode op elk stembiljet, van de uitgebrachte stemmen op de gegevensdrager van het stembureau, de correcte registratie van de

mémoire provenant du bureau de vote sur le support de mémoire destiné à la totalisation des votes et la totalisation des suffrages exprimés. Ils peuvent également vérifier la fiabilité des logiciels de transmission digitale des résultats électoraux.

Le Collège d'Experts peut procéder à un audit des résultats afin de garantir la fiabilité et l'intégrité du système de vote électronique avec production d'un bulletin de vote en papier.

Ils effectuent ce contrôle à partir du quarantième jour précédant l'élection, le jour de l'élection et après celle-ci, jusqu'au dépôt du rapport visé au § 2.

§ 2. Au plus tard quinze jours après la clôture des scrutins et en tout état de cause avant la validation des élections pour ce qui concerne la Chambre des représentants, les Parlements de communauté et de région et le Parlement européen, les experts remettent un rapport au ministre de l'Intérieur ainsi qu'aux assemblées législatives fédérales, régionales et communautaires. »

Conformément à l'article 35 de la loi du 7 février 2014, le Collège assure cette mission tant pour le vote électronique avec preuve papier (système SmartMatic) que pour le vote automatisé, réglé par la loi du 11 avril 1994 organisant le vote automatisé (système Jites / Digivote).

Par rapport aux élections de 2012, la mission du Collège a été étendue notamment aux tâches suivantes :

- le contrôle de la préparation, de l'utilisation et du bon fonctionnement des matériels, logiciels et procédures de transmission et de diffusion digitale des résultats ;
- la réalisation d'un audit des résultats afin de garantir la fiabilité et l'intégrité du système de vote.

gegevensdrager van het stembureau op de gegevensdrager bedoeld voor het optellen van de stemmen en de totalisering van de uitgebrachte stemmen. Ze kunnen eveneens de betrouwbaarheid nagaan van de software voor het digitaal doorsturen van de verkiezingsuitslagen.

Het College van Deskundigen kan overgaan tot een audit van de uitslagen om de betrouwbaarheid en integriteit van het elektronische stelsysteem met afdruk van een papieren stembiljet te verzekeren.

Zij verrichten de controle vanaf de veertigste dag voor de verkiezing, op de verkiezingsdag zelf en hierna tot de indiening van het in § 2 bedoelde verslag.

§ 2. Uiterlijk vijftien dagen na de sluiting van de stemming en in ieder geval voor de geldigverklaring van de verkiezingen voor wat de Kamer van volksvertegenwoordigers, de Gewest- en Gemeenschapsparlamenten en het Europees Parlement betreft, bezorgen de deskundigen een verslag aan de minister van Binnenlandse Zaken, alsook aan de federale wetgevende assemblees en de Gewest- en Gemeenschapsparlamenten."

Overeenkomstig artikel 35 van de wet van 7 februari 2014, vervult het College deze opdracht zowel voor de elektronische stemming met papieren bewijsstuk (systeem SmartMatic) als voor de geautomatiseerde stemming, die geregeld wordt bij de wet van 11 april 1994 tot organisatie van de geautomatiseerde stemming (systeem Jites / Digivote).

Ten opzichte van de verkiezingen van 2012 werd de opdracht van het College uitgebreid met onder meer de volgende bevoegdheden:

- het controleren van de voorbereiding, het gebruik, en de goede werking van de hardware, software en procedures voor de digitale transmissie en het digitaal verspreiden van de resultaten;
- het uitvoeren van een audit van de uitslagen om de betrouwbaarheid en integriteit van het stelsysteem te verzekeren.

2.4.2 La nature de la mission : collecte d'informations et contrôle De aard van de opdracht: informatieverzameling en controle

Il ressort de ce qui précède que la mission du Collège consiste essentiellement à exercer un contrôle à l'égard du vote électronique avec preuve papier et du vote automatisé, pendant la préparation des élections, le jour du scrutin et durant la période qui suit, jusqu'au dépôt de son rapport.

Pour pouvoir mener à bien cette mission, le Collège reçoit du ministre de l'Intérieur ou de son délégué,

Uit het bovenstaande blijkt dat de opdracht van het College in wezen bestaat in het uitoefenen van controle op de elektronische stemming met papieren bewijsstuk en op de geautomatiseerde stemming tijdens de voorbereiding van de verkiezingen, op de verkiezingsdag, en daarna tot de indiening van zijn verslag.

Teneinde deze opdracht te kunnen uitoefenen, ontvangt het College het nodige materiaal alsook alle

des membres de bureaux électoraux, des organismes d'avis et des entreprises privées associées au déroulement du processus électoral le matériel ainsi que l'ensemble des données, renseignements et informations utiles (article 25, § 1er, alinéa 2, de la loi du 7 février 2014).

Pendant la préparation des élections, le jour du scrutin ou durant la période qui précède le dépôt de son rapport, il n'appartient toutefois pas au Collège de donner des avis aux acteurs associés au processus électoral, qu'il s'agisse des différents bureaux électoral, qu'il s'agisse des différents bureaux (bureaux de vote, bureaux principaux de canton, etc.), du ministre de l'Intérieur, du SPF intérieur ou des entreprises privées qui ont produit le matériel requis ou ont été consultés dans ce cadre. Il n'entre pas non plus dans la mission légale du Collège de donner son accord, durant sa période d'activité, sur une quelconque matière, y compris celles relevant de sa mission, à l'intention de l'un ou l'autre de ces acteurs. S'il en était décidé autrement, et si le Collège intervenait activement durant cette période, il ne serait en effet plus à même d'assurer sa mission légale de contrôle en toute indépendance.

Le Collège ne transmet un relevé de ses conclusions et ne formule d'éventuelles recommandations que dans le présent rapport, qu'il rédige à l'intention du ministre de l'Intérieur ainsi que des assemblées législatives fédérales, régionales et communautaires en conclusion de sa mission.

nuttige gegevens, inlichtingen en informatie van de minister van Binnenlandse Zaken of zijn afgevaardigde, van de leden van de kiesbureaus en van de adviesorganen en privébedrijven die bij het kiesproces zijn betrokken (artikel 25, § 1, tweede lid, van de wet van 7 februari 2014).

Het komt echter niet toe aan het College om gedurende de voorbereiding van de verkiezingen, op de verkiezingsdag of in de periode tot de indiening van zijn verslag adviezen te verstrekken aan de actoren die bij het kiesproces betrokken zijn, ongeacht of het daarbij gaat om de onderscheiden bureaus (stembureaus, kantonhoofdbureaus, etc.), de minister van Binnenlandse Zaken, de FOD Binnenlandse Zaken, of de privébedrijven die het benodigde materiaal hebben geproduceerd of erover advies hebben verleend. Het behoort evenmin tot de wettelijke opdracht van het College om tijdens de periode van zijn werkzaamheden in enige aangelegenheid met inbegrip van de aangelegenheden die tot de opdracht van het College behoren zijn goedkeuring te verlenen ten overstaan van één of meerdere van deze actoren. Indien men er anders over zou oordelen, en het College actief zou optreden gedurende deze periode, zou het College immers niet langer op een onafhankelijke manier zijn wettelijke controleopdracht kunnen vervullen.

Slechts in het voorliggende verslag, dat het College tot besluit van zijn opdracht opstelt ten behoeve van de minister van Binnenlandse Zaken, van de federale wetgevende assemblees en van de Gewest- en Gemeenschapsparlamenten, geeft het College een overzicht van zijn bevindingen en doet het eventuele aanbevelingen.

3 Description des systèmes de vote automatisé

Deux systèmes sont déployés dans le cadre de ces élections. Dix-sept communes bruxelloises et les communes automatisées en Région wallonne utilisent le système Jites-Digivote, tandis que deux communes bruxelloises (Saint-Gilles et Woluwe-Saint-Pierre) et les communes automatisées en Région flamandes utilisent le nouveau système développé par la société SmartMatic.

3.1 Le vote automatisé sans preuve papier (Jites / Digivote)

Le système de vote sans preuve papier a été largement décrit dans les rapports des Collèges d'experts des élections antérieures. Il n'est par conséquent plus détaillé dans cette édition. Seules les différences sont relevées ci-dessous.

Deux différences sont à souligner par rapport aux élections de 2010 et de 2012. La première provient du nombre d'élections. Pour la première fois, 3 ou 4 scrutins ont été simultanément organisés, ce qui a exigé une réorganisation du contenu des cartes magnétiques et a rendu sa gestion nettement plus complexe.

La seconde différence est que cette version intègre une amélioration de l'ergonomie du système de vote : lorsqu'un électeur a sélectionné un candidat ou la case de tête et qu'il veut modifier son choix, il ne doit plus,

comme c'était le cas auparavant, revenir à l'écran précédent de sélection des listes. Il lui suffit de re-cliquer sur le même candidat ou la case de tête pour le désélectionner. Cette fonctionnalité avait déjà été introduite lors d'élections précédentes, mais supprimée en 2010 et 2012.

C'est cette amélioration qui, en raison d'une erreur dans sa programmation, va bloquer la chaîne d'enregistrement des disquettes et entraîner la perte de votes pourtant correctement attribués par les électeurs.

Comme pour les systèmes Jites utilisés lors des élections communales, la totalisatrice spécifique a été remplacée par le système PGM3 de CODI.

3.2 Le vote automatisé avec preuve papier (SmartMatic)

3.2.1 Les systèmes

La machine à voter SmartMatic est un ordinateur standard (quant à ses composants) avec un boîtier particulier muni d'un écran tactile, d'un lecteur de cartes à puce (ou smartcard) et d'une imprimante intégrée. L'interrupteur, la prise pour le raccordement au réseau électrique, la prise pour le clavier, les connecteurs USB, le connecteur pour l'alarme sont situés sur la face arrière. Les seuls composants de l'ordinateur auquel l'électeur a accès sont le lecteur de carte à puce et l'imprimante qui sont sur la face avant. Une machine à voter n'a ni clavier ni disque dur.

La machine du président est constituée d'un ordinateur de type « portable » auquel sont connectés un hub USB muni de deux clés USB identiques, une urne électronique et un lecteur-enregistreur de cartes à puces. Les clés USB contiennent tous les logiciels du bureau de vote (machine du président et machines à voter) et du bureau principal (totalisation). L'urne est composée d'un réservoir destiné à collecter les votes imprimés par les machines à voter et est surplombé par un scanner de QR-codes (code-barres bidimensionnel).

3.2.2 La procédure électorale avec preuve papier

3.2.2.1 L'ouverture du bureau de vote avec preuve papier

La première opération consiste à démarrer la machine du président à l'aide des deux clés USB identiques qui lui ont été fournies en même temps que ses mots de passe.

Le président et son bureau vérifient le bon raccordement des différents éléments et démarrent la machine du président. Ensuite vient une phase de diagnostic de la machine du président et des périphériques (clés USB, urne, valideuse de carte à puce, clavier, souris,...) raccordés. Un rapport de diagnostic est imprimé.

La machine du président demande de démarrer les machines à voter. Une des clés USB est nécessaire pour démarrer les machines à voter. Lorsque toutes les machines à voter sont prêtes, les clés USB sont réintroduites dans la machine du président.

3.2.2.2 Le déroulement du vote

Le vote est réalisé sur la machine à voter qui se trouve dans l'isoloir. La machine à voter imprime une preuve papier reprenant le vote sous forme lisible ainsi que sa représentation sous forme de QR-code.

Chaque électeur reçoit une carte à puce initialisée selon le type d'électeur: national, européen, belge résident à l'étranger. Il l'emporte dans l'isoloir et l'introduit dans la machine à voter. Toute carte mal initialisée, non initialisée ou déjà utilisée 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 sur l'écran tactile, il doit le confirmer. À partir de ce moment, le vote est définitif. Tant qu'il n'est pas confirmé, l'électeur peut annuler son vote et recommencer.

Après confirmation du vote, la machine à voter imprime le vote sous forme textuelle ainsi que sous la forme d'un QR-code sur un bulletin « preuve papier » et invite l'électeur à retirer la carte à puce. Dans un isoloir prévu à cet effet, l'électeur peut scanner le QR-code de sa preuve papier au moyen d'un scanner portable. Le contenu du QR-code est alors affiché à l'écran et l'électeur peut vérifier son vote.

Après avoir exprimé son vote dans l'isoloir, l'électeur scanne le QR-code de sa preuve papier au moyen du scanner qui se trouve au-dessus de l'urne. Après confirmation sonore et visuelle (sur l'écran du président) que le QR-code a bien été lu et enregistré par l'ordinateur du président, l'électeur introduit sa preuve papier dans l'urne.

3.2.2.3 La clôture du bureau de vote

A l'issue du scrutin, le bureau de vote est clôturé et un document reprenant les chiffres-clés est imprimé. L'urne est ouverte et les bulletins « preuves papiers » sont transférés dans une enveloppe qui est scellée. Le procès-verbal, les clés USB du bureau et l'enveloppe scellée contenant les preuves papiers sont emmenés au bureau principal.

3.2.2.4 Différences avec le système utilisé lors des élections de 2012

Le système de totalisation spécifique a été abandonné au profit d'un système de totalisation capable de totaliser tant les disquettes issues de Jites que les clés USB issues de SmartMatic (voir la description plus bas). A la clôture des opérations de votes, le système crée un répertoire appelé EXPORT sur les clés USB. Ces répertoires contiennent sous une forme cryptée, toutes les données nécessaires à la totalisation.

Het systeem dat gebruikt werd voor de totalisatie heeft plaatsgemaakt voor een systeem dat zowel de gegevens van de diskettes (Jites) als de gegevens van de USB-sticks (SmartMatic) kan verwerken (zie beschrijving verderop). Bij het afsluiten van de stemverrichtingen creëert het systeem een map EXPORT op de USB-stick. Deze mappen bevatten, geëncrypteerd, alle gegevens nodig voor de totalisatie.

Les principales différences par rapport à la situation de 2012 sont résumées ci-dessous :

Hieronder worden de voornaamste verschilpunten met de situatie uit 2012 opgesomd:

- le démarrage d'un bureau de vote est nettement plus rapide et plus simple ;
- le mode test lors de la procédure de démarrage a été abandonné pour éviter les erreurs ;
- après la sélection d'une liste, une confirmation est obligatoire en bas à droite avant de passer à la liste des candidats ce qui rend impossible la sélection involontaire de candidats ;
- de petites adaptations ont été faites pour augmenter l'ergonomie du système ;
- le nombre de cas où une alarme se déclenche a été fortement réduit ;
- l'urne enregistre correctement le vote, quel que soit l'écran affiché sur la machine du président corrigeant ainsi un problème détecté lors des élections de 2012.

- de opstart van een kiesbureau is significant sneller en veel eenvoudiger geworden;
- de testmodus tijdens de opstartprocedure werd weggelaten teneinde fouten te vermijden;
- na het selecteren van een kieslijst is er een verplichte bevestiging onderaan rechts op het scherm nodig om de kandidaten van de lijst te zien waardoor onbedoelde keuze van een kandidaat niet langer mogelijk is;
- er werden kleine aanpassingen gedaan om de ergonomie van het systeem te verbeteren;
- het aantal gevallen waarin een alarm wordt gegenereerd is significant verminderd;
- de urne verwerkt de stem correct, ongeacht het scherm waarin de voorzittersmachine zich bevindt. Dit corrigeert een probleem ontdekt tijdens de verkiezingen van 2012.

3.3 Le système CODI

Codi désigne l'ensemble des logiciels installés dans les bureaux principaux et sur les serveurs centraux du SPF Intérieur. Au niveau des bureaux principaux, il s'agit des logiciels PGM2 et PGM3. Sur les serveurs centraux, il s'agit des logiciels LOC1 et LOC2. Le Collège ne s'est intéressé dans le cadre de ces élections qu'aux logiciels PGM2 et PGM3.

Dans le cadre des élections électroniques, le logiciel **PGM3** est chargé de :

- récolter les disquettes (Jites) et les clés usb (SmartMatic) en provenance des bureaux de vote ;
- totaliser les résultats des bureaux de vote ;
- générer, signer numériquement et envoyer les pv des bureaux de canton ;
- transférer les résultats vers les serveurs centraux au fur et à mesure de la récolte des supports.

Le système **PGM3** est installé sur une machine Windows 7 avec des accès très restreints pour les opérateurs. Le système **PGM2** regroupe pour sa part les résultats des votes électroniques et des votes papier. C'est à ce

niveau que les résultats de bureaux de dépouillement sont encodés et que les corrections de bureaux de canton peuvent être encodées. **PGM3/2** calcule ensuite la répartition des sièges, produit les PV, permet de les signer numériquement et les envoie vers les serveurs centraux.

Le système PGM2 est installé sur une machine Windows 7 standard.

3.4 Le système DePass – E-counting

Le système DEPASS (DEPouillement ASSisté) est un système destiné à faciliter le dépouillement papier. Deux PCs reliés en réseau sont utilisés pour procéder à un double encodage de tous les bulletins d'un bureau de dépouillement. Ces PCs sont dotés d'un écran tactile et exécutent sous Windows7 un logiciel convivial. Ce logiciel permet de choisir une liste et ensuite de sélectionner les candidats. Après validation du bulletin encodé, le système affiche à nouveau l'écran des listes électorales, avec pour chaque liste, le chiffre électoral total qu'elle a atteint. Le double encodage des bulletins doit se faire dans le même ordre ce qui permet au système de détecter les erreurs d'encodage. Des fonctions avancées permettent d'afficher l'ensemble des bulletins encodés.

Le double encodage se fait au moyen de deux équipes de deux personnes. Dans chaque équipe, l'une dicte le bulletin de vote et l'autre l'encode. Le système empêche une équipe de prendre trop d'avance sur la seconde, en limitant l'écart entre les deux PCs (option paramétrable).

3.5 Le système Web2

Un nouveau logiciel de type WEB, nommé **WEB2** et hébergé sur un serveur du SPF Intérieur, a été utilisé afin de permettre l'encodage des votes des belges à l'étranger ayant votés personnellement ou par procuration au sein des 120 postes diplomatiques et consulaires pour les élections de La Chambre (types de vote E3 et E4).

L'encodage des votes via l'application WEB2 a été réalisé le samedi précédant le jour des élections en Belgique à partir de 20 postes diplomatiques (bureaux régionaux de dépouillement) où avaient été centralisés les votes papiers. Le réseau Intranet du SPF Affaires étrangères et une connexion sécurisée du SPF Affaires Etrangères vers le SPF Intérieur ont été utilisés pour accéder à l'application WEB2.

Les données des votes, cryptées et sauvegardées sur le serveur, ont été décryptées le dimanche, jour des élections en Belgique.

4 Contrôles et constatations

4.1 Contrôles effectués avant le jour des élections

4.1.1 La certification des logiciels électoraux

4.1.1.1 Application de la législation

L'article 4, § 3, de la loi du 7 février 2014 dispose que tous les systèmes de vote et de dépouillement électronique avec preuve papier, les systèmes de totalisation électroniques des votes doivent être agréés par le ministre de l'Intérieur.

L'organisme chargé de remettre les avis est la société PricewaterhouseCoopers.

Le Collège était présent lors de la remise des rapports d'avis au SPF Intérieur et a reçu une copie de ceux-ci.

La ministre de l'Intérieur a agréé tous les systèmes de vote et de dépouillement électroniques sur la base des avis émis.

4.1.1.2 Certifications

Le 4 avril 2014, la société PricewaterhouseCoopers, organisme d'avis agréé par le SPF Intérieur et mandaté par la société Stésud, a présenté au SPF Intérieur et au Collège d'experts son rapport d'« *Evaluation des systèmes de vote électronique (Jites) en vue des élections européennes, fédérales et régionales de mai 2014* ».

Un rapport équivalent sur le système SmartMatic a été présenté le même jour.

Le 30 avril 2014, le rapport sur les systèmes des bureaux principaux et des serveurs centraux (CODI), celui

sur le système Web2 destiné à l'enregistrement des votes à l'étranger et celui sur le système Depass de dépouillement assisté des votes papier ont été remis aux différentes parties intéressées. Ces rapports visaient à vérifier l'adéquation des applications pour la multiple élection du 25 mai 2014. Les aspects étudiés couvraient à la fois la conformité à la législation électorale, la fiabilité et la qualité des applications. Les sous-systèmes de préparation des supports des bureaux de vote étaient également étudiés dans ces rapports.

4.1.1.3 Rapport sur les systèmes Jites

Les versions testées des logiciels portent les numéros de version suivants :

- PREP v. 14.50 : préparation des listes et des supports
- MAV v. 9.16 : logiciel de la machine à voter
- URN v. 9.15 : logiciel de l'urne

4.1.1.3.1 Dépôt des sources au coffre

Une enveloppe scellée contenant les sources des logiciels, les programmes exécutables et les fichiers de données propres à l'élection a été déposée au coffre du SPF Intérieur (banque Belfius) en présence de tous les intervenants. Le Collège n'a cependant pas pu prendre connaissance du contenu de l'enveloppe qui avait été préalablement scellée. Ce point a été indiqué au PV.

Le Collège a reçu une copie de l'ensemble des sources et a pu vérifier ultérieurement que les codes sources Jites étudiés par PricewaterhouseCoopers étaient identiques.

4.1.1.3.2 Avis de PricewaterhouseCoopers

PricewaterhouseCoopers donne un avis globalement positif et dit être en mesure de conclure, avec une assurance raisonnable que l'application est compatible avec le matériel, qu'elle satisfait aux exigences de la législation et qu'elle est fiable et adéquate.

Au cours de sa mission, PricewaterhouseCoopers a formulé des observations qu'elle a considérées comme bloquantes et qui ont nécessité des adaptations par Stésud. Ces adaptations, assez mineures, concernaient essentiellement des erreurs linguistiques, des erreurs dans les logos ou encore des omissions dans les PV générés. Rien par contre n'a été signalé au niveau des fonctionnalités de l'application proprement dite.

PricewaterhouseCoopers a formulé d'autres observations, concernant notamment la qualité du code source et des manuels d'utilisation. Ces observations n'ont pas été considérées comme bloquantes et n'ont pas donné lieu à des adaptations.

4.1.1.4 Rapport sur les systèmes SmartMatic

Les versions testées des logiciels portent les numéros de version suivants :

- ECM v. 2.0.5_5.20140303.1209.1123 : préparation des listes et des supports
- VOTE v. 1.7.21 : logiciels des bureaux de vote

4.1.1.4.1 Dépôt des sources au coffre

Comme lors de la certification des logiciels Jites, une enveloppe scellée contenant les sources des logiciels, les programmes exécutables et les fichiers de données propres à l'élection a été déposée au coffre du SPF Intérieur (banque Belfius) en présence de tous les intervenants. Dans ce cas non plus, le Collège n'a pu prendre connaissance du contenu de l'enveloppe qui avait été préalablement scellée. Ce point a été indiqué au PV.

Le Collège a reçu une copie de l'ensemble des sources mais n'a pas été en mesure de vérifier ultérieurement que les codes sources étudiés par PricewaterhouseCoopers étaient identiques.

4.1.1.4.2 Avis de PricewaterhouseCoopers

PricewaterhouseCoopers donne un avis détaillé et globalement positif sur le système SmartMatic. PricewaterhouseCoopers dit être en mesure de conclure, avec une assurance raisonnable que l'application est compatible avec le matériel, qu'elle satisfait aux exigences de la législation et qu'elle est fiable et adéquate.

Au cours de la phase de test, une légère adaptation a été apportée à l'application suite aux remarques de PricewaterhouseCoopers.

Quelques observations non bloquantes ont été formulées dans le rapport de PricewaterhouseCoopers, entre autre :

- documentation lacunaire des codes sources ;
- quelques erreurs linguistiques dans les applications (invisibles pour l'électeur) ;
- la possibilité de vérifier son vote à l'aide d'un lecteur de codes-barres n'est pas clairement expliquée à l'électeur ;
- les caractères utilisés pour imprimer les bulletins sont peu lisibles.

4.1.1.5 Rapport sur les systèmes CODI

Les versions testées des logiciels portent les numéros de version suivants :

- PGM2 v. 275 du 25 avril 2014 : totalisatrices des bureaux de vote papier et des bureaux principaux des niveaux supérieurs
- PGM3 v. 1.66b du 17 avril 2014 : totalisatrices des bureaux de vote et de dépouillement automatisés
- LOC1 et LOC2 v. 4.28 du 29 avril : collecte des résultats et calculs au niveau des serveurs centraux

Les analyses de PricewaterhouseCoopers ont conduit à plusieurs adaptations par Stésud avant de donner satisfaction : corrections linguistiques, amélioration des messages d'erreurs, vérification de l'intégrité des fichiers critiques.

Avis de PricewaterhouseCoopers

PricewaterhouseCoopers donne un avis globalement positif et dit être en mesure de conclure, avec une assurance raisonnable que l'application est compatible avec le matériel, qu'elle satisfait aux exigences de la législation et qu'elle est fiable et adéquate.

PricewaterhouseCoopers fait cependant remarquer que des lacunes dans le code électoral empêchent de déterminer si le logiciel, dans certains cas limites, se comporte adéquatement.

4.1.1.6 Rapport sur le système Web2

Ce système permet l'encodage et le transfert des résultats des électeurs belges ayant voté à l'étranger.

La version testée du logiciel porte le numéro de version *Web2 1.0.5* et est datée du 29 avril 2014.

A nouveau, les analyses de PricewaterhouseCoopers ont conduit à plusieurs adaptations par Stésud avant de donner satisfaction : corrections linguistiques, amélioration de la logique, ajout de verrous avant clôture, amélioration des messages d'erreurs, et quelques autres erreurs fonctionnelles plus importantes.

Avis de PricewaterhouseCoopers

A l'issue du processus d'analyse/amélioration, PricewaterhouseCoopers donne un avis globalement positif et dit être en mesure de conclure, avec une assurance raisonnable que l'application satisfait aux exigences de la législation et qu'elle est fiable et adéquate.

PricewaterhouseCoopers émet cependant quelques remarques complémentaires qui peuvent être compensées par les procédures, notamment en matière de sécurité (nombre d'essais de mot de passe non limité).

4.1.1.7 Rapport sur le système Depass

Ce système est un outil de dépouillement assisté par ordinateur.

La version testée du logiciel porte le numéro de version *Depass v. 1.34*, datée du 18 février 2014.

Avis de PricewaterhouseCoopers

A l'issue de son analyse, PricewaterhouseCoopers donne un avis globalement positif et dit être en mesure de conclure, avec une assurance raisonnable que l'application satisfait aux exigences de la législation et qu'elle est fiable et adéquate.

PricewaterhouseCoopers liste quelques faiblesses pouvant être compensées par des procédures (absence de logiciel antivirus, clôture précoce possible, manque de sécurisation des répertoires et du système Windows,...).

Stésud présent lors de la présentation a répondu aux remarques en matière de sécurité en insistant sur le fait que les PC étaient livrés par Stésud, n'étaient pas en réseau et étaient en permanence sous le contrôle du bureau de dépouillement).

PricewaterhouseCoopers fait également quelques remarques non bloquantes pouvant être corrigées dans une édition ultérieure (corrections d'interface et linguistiques).

4.1.2 Le système SmartMatic

Au moyen d'un matériel de démonstration mis à sa disposition, le Collège a procédé à divers simulations d'opérations de vote (démarrage, d'un bureau, émission de votes, enregistrements de votes, clôture du bureau). Pour cela, le Collège a reçu du SPF Intérieur des jeux de clés USB pour un bureau du canton d'Anvers et un bureau du canton de Bruxelles. Il a récupéré les résultats générés sur les clés USB et les a contrôlés. Aucune discordance n'est apparue avec les résultats attendus.

Pendant ces tests, le Collège a vérifié que les recommandations formulées dans les précédents rapports à propos du système SmartMatic ont été prises en considération.

Le Collège a reçu de la société SmartMatic deux logiciels de décryptage des données des clés USB clôturées. Le premier permet le décryptage des fichiers d'exportation qui sont exploitées par le logiciel de totalisation. Le Collège n'a pas reçu le code source de ce logiciel et n'a donc pas pu le contrôler. Lors de l'utilisation de ce logiciel, le Collège n'a pas constaté de problèmes de déchiffrement des données.

Le second logiciel permet le décryptage des votes individuels. Le Collège a pu constater que ce logiciel était identique à celui mis à disposition lors des élections de 2012. Le Collège n'en pas reçu le code source non-plus. Il a cependant pu constater qu'il s'agissait du même logiciel qu'en 2012 et dont les membres du Collège bruxellois pour cette élection avaient les sources. Le Collège a donc opté pour l'utilisation de ce logiciel pour ces contrôles après les élections.

4.1.3 Le système Jites

Le Collège a reçu du SPF Intérieur différents jeux de disquettes pour des bureaux de vote des cantons de Bruxelles, Liège et Eupen. Avec le matériel Jites et Digivote mis à sa disposition, le Collège a procédé à différentes simulations d'opérations de vote (démarrage d'un bureau, émission de votes, enregistrements de votes, clôture du bureau). Il a récupéré les résultats générés sur les disquettes et les a contrôlés. Aucune discordance n'est apparue avec les résultats attendus.

Le Collège a également pu lire les cartes magnétiques au moyen d'un matériel et d'un logiciel tout à fait indépendant de celui des systèmes Jites/Digivote. Cette opération s'est révélée cruciale pour les analyses qui ont été réalisées à propos du « bug des élections 2014 ».

4.1.4 Le système CODI

Le Collège d'experts a concentré son attention sur le logiciel de totalisation PGM3 qui est un des composants du système CODI. La société Stésud a fourni au Collège un PC de totalisation et des jeux de données fictives pour faire la démonstration du système. Le Collège a ainsi pu constater le fonctionnement de l'application PGM3.

Il est à noter que les systèmes PGM3 et PGM2 (totalisation dans les cantons votant traditionnellement et dans les bureaux de circonscription) sont installés sur des PC standards sous Windows, configurées de manière standard et sans aucune mesure particulière de protection. Il n'y a aucun antivirus, anti-malware ou pare-feu spécifique. Comme ces PC sont installés plusieurs jours avant les élections dans des locaux où des connexions Internet classiques sont disponibles, il y a un risque bien réel au niveau de la sécurité.

Dans le cas spécifique de la Communauté germanophone la mauvaise qualité de la traduction des messages d'erreur est à déplorer. Certains présidents de bureau de totalisation ont rencontré des problèmes de droits d'utilisation lors de la validation et de la signature électronique du PV. Ces problèmes pouvaient être réglés à court terme par Stésud.

4.1.5 Confection des supports mémoires – Vervaardiging van de geheugendragers

Le 14 mai 2014, le Collège a visité les locaux où tous les supports informatiques utilisés pour les élections ont été confectionnés tant pour les systèmes SmartMatic que Jites. Dans le cas du système Jites il s'agit des disquettes et des enveloppes contenant les mots de passe. Dans le cas du système SmartMatic, il s'agit des clés USB et des enveloppes contenant les mots de passe. Le couloir reprenant tous les locaux de confection est sécurisé via un système de badge, un garde et des caméras. Les locaux individuels sont fermés à clé. Le personnel chargé de la confection des supports et de l'impression des mots de passe est du personnel propre au ministère de l'intérieur. Notons toutefois qu'un copieur/fax est présent dans les locaux, mais également que les téléphones portables étaient autorisés.

Op 14 mei 2014 heeft het College de lokalen bezocht waar alle informatiedragers vervaardigd zijn die gebruikt worden voor de verkiezingen, en dit zowel voor de SmartMatic als voor de Jites systemen. In het geval van het Jites systeem gaat het om de diskettes en de enveloppes met de wachtwoorden. In het geval van het SmartMatic-systeem gaat het om de USB sleutels en de enveloppes met de wachtwoorden. De gang waarrond zich de lokalen voor de aanmaak bevinden, is beveiligd door een badgesysteem, een bewaker en cameras. De individuele lokalen voor de aanmaak zijn op slot. Het personeel dat instaat voor de aanmaak van de diskettes en voor het afprinten van de paswoorden is eigen personeel van de FOD BiZa. Wij noteren echter de aanwezigheid van een copier/fax, maar ook het feit dat draagbare telefoons toegelaten werden in de lokalen.

4.1.6 Participation aux séances de formations des présidents de bureaux de vote

Les membres du Collège ont assisté à un certain nombre de formations de présidents.

Le Collège a par le passé régulièrement fait la remarque que les instructions fournies par le SPF Intérieur pour les présidents des bureaux de votes étaient longues et n'étaient pas structurées. Ces instructions étaient souvent changées in extrémis. Le Collège avait pu constater que pour ces différentes raisons, les instructions complètes n'étaient pas ou peu utilisées lors des formations.

Le Collège a noté que pour les élections de 2014, ces instructions avaient été totalement réécrites. Ces nouvelles instructions sont claires, simplifiées et publiées sur le site web du SPF plusieurs semaines avant le début des élections. Sur le site web des élections se trouvaient également des films expliquant entre-autre clairement le fonctionnement d'un bureau de vote SmartMatic.

Sur base de ces nouvelles instructions, le Collège a établi un questionnaire pour vérifier si les différents points repris dans les instructions du SPF étaient mentionnés et expliqués.

Le Collège a malheureusement dû constater qu'à nouveau certaines communes ont pris beaucoup de liberté par rapport aux instructions du SPF.

Le jour des élections les différents contrôles dans les bureaux de vote ont permis de vérifier que les instructions du SPF n'avaient pas toujours été suivies par les présidents.

Les formations ont été suivies à Wetteren, Eupen, St-Vith, Kraainem, Wezembeek-Oppem, Molenbeek-Saint-Jean, St-Josse-ten-Node, Heverlee, Zoutleeuw, Aalst, Liedekerke et Woluwe-Saint-Pierre. Le détail des observations est repris dans les annexes du rapport.

4.1.7 Authenticité des codes sources

4.1.7.1 Jites

Le Collège a pu vérifier que le code source reçu du SPF Intérieur est identique à celui qui avait été remis à PWC pour sa mission de certification et qui a été publié sur le site des élections.

Le Collège a également procédé à une recompilation et a pu vérifier qu'il obtenait les mêmes exécutables (avec exceptionnellement quelques différences inhérentes à des recompilations dans des environnements différents).

4.1.7.2 SmartMatic

Le Collège a reçu une copie du code source. Il n'a pas eu le temps de l'analyser et a décidé de laisser cette

tâche au Collège permanent. Le Collège a pu vérifier que le code source reçu du SPF Intérieur est identique à celui qui a été publié sur le site des élections.

4.1.8 Analyse des codes sources

4.1.8.1 Jites

Le Collège a comparé la version 2014 des codes sources du logiciel Jites avec ceux des élections antérieures. Les différences étant relativement importantes, le Collège n'a pas eu le temps d'approfondir cette comparaison et a préféré se pencher de manière plus approfondie sur le « bug de l'élection 2014 ». La partie du code source à l'origine du bug est analysée et expliquée dans le chapitre qui lui est consacré.

4.1.8.2 SmartMatic

Le Collège a comparé la version 2014 des codes sources du logiciel SmartMatic avec ceux des élections de 2012. Les différences sont très importantes : le Collège n'a pas eu le temps d'approfondir cette analyse et laisse cette tâche au Collège permanent.

4.1.9 Sécurité des systèmes

4.1.9.1 Usage de la cryptographie

Le Collège d'experts a analysé la manière dont la sécurité informatique est mise en œuvre dans les différents systèmes. Cette analyse s'est faite partiellement sur base du code source des systèmes de votes mais surtout sur base des documents produits par Stésud et SmartMatic décrivant la sécurité de leurs systèmes.

Sur cette base le collège d'experts a mis en évidence l'usage de certains standards cryptographiques dépassés, la nécessité d'établir une politique de gestion claire et uniforme des différents mots de passe utilisés sur les systèmes ainsi que des clés cryptographiques manipulées, la nécessité de mettre systématiquement en place des canaux de communications sécurisés (à savoir chiffrés mais aussi authentifiés, garantissant la non-répudiation et l'intégrité).

Le collège d'experts suggère aussi des mesures (sur base de réalisations systématiques d'audits, de relectures systématiques des votes par les électeurs, de norme de qualité des codes sources et de la documentation) afin de garantir plus de transparence, de confiance et de sécurité dans le processus électoral.

Het College van deskundigen heeft de informaticabeveiliging van de verschillende systemen geanalyseerd. Deze analyse gebeurde deels op basis van de broncode van de stelsystemen, maar vooral op basis van de veiligheidsdocumentatie opgesteld door Stésud en SmartMatic.

Op basis hiervan heeft het College van deskundigen het gebruik van voorbijgestreefde cryptografische standaarden aan het licht gebracht, alsook de noodzaak om een duidelijke en uniforme beheerspolitiek te hanteren voor zowel de paswoorden gebruikt in de verschillende systemen als de gebruikte cryptografische sleutels, de noodzaak om systematisch beveiligde communicatiekanalen te gebruiken (niet alleen geëncrypteerd, maar ook geauthenticeerd om onweerlegbaarheid en integriteit te garanderen).

Het College van deskundigen suggereert ook maatregelen te nemen om meer transparantie, betrouwbaarheid en veiligheid te garanderen in het verkiezingsproces (op basis van systematische audits, de kiezer systematisch zijn stem laten herlezen, kwaliteitseisen op te leggen voor de broncode en de documentatie).

Le Collège d'experts constate que des clés AES (de 256 bits) sont dérivées de mots de passe (mots de passe de présidents, mot de passe du "recount", ...). Ces mots de passe sont de 16 caractères exclusivement alphabétiques ce qui représente moins de 2^{96} possibilités et donc une source d'entropie beaucoup plus faible que les 256 bits attendus.

Le Collège d'experts constate qu'il a été difficile d'obtenir des réponses complètes aux différentes questions posées à la société Stésud.

4.1.9.2 Analyse automatisée des vulnérabilités

Met behulp van Stésud, FOD Binnenlandse Zaken en het CIBG werden uit een aantal technische netwerk schema's een aantal publieke IP-adressen geïdentificeerd. Er dient evenwel gezegd dat de beschikbare informatie fragmentair en onvolledig was. Zo heeft Buitenlandse Zaken geen informatie verstrekt over de verbindingen vanuit de ambassades. Wel werd geconstateerd dat deze verbindingen gebeurden vanaf verouderde XP PCs. Er was bovendien geen mogelijkheid om de IP-adressen uit de technische schema's te identificeren volgens type van netwerkapparatuur. Achter deze IP-adressen zaten servers en firewalls die toegankelijk waren vanaf het Internet. Kwetsbaarheden op deze toestellen zouden de veiligheid van het netwerk kunnen compromitteren.

Om deze kwetsbaarheden (zoals verouderde operating systems, bugs, onzorgvuldige configuraties, ontbrekende updates of patches, enz.) te kunnen detecteren en identificeren werd door het CIBG aan het College een professionele tool ter beschikking gesteld om deze publieke ip-adressen te testen. Deze tool maakt gebruik van niet-intrusieve of storende methodes en kon het verkiezingsnetwerk op geen enkel moment onderbreken of vertragen. Desalnietemin werd IBZ op de hoogte gebracht van deze technische actie voor de aanvang van de geautomatiseerde scans.

Tijdens de testen uitgevoerd van 22 mei 2014 tot 27 mei 2014 werden slechts 2 hosts geïdentificeerd die zichtbaar waren vanaf het internet. De regelmatig herhaalde scans toonden evenwel geen enkele zichtbare vulnerabiliteit. Het College kan daardoor veronderstellen dat de actieve preventieve veiligheidsmaatregelen om onrechtmatige toegang tot het netwerk te verhinderen leken te volstaan om de veiligheid van het netwerk te garanderen. Om met meer zekerheid te kunnen concluderen dat de veiligheidsmaatregelen volstonden zouden meer tools en middelen ter beschikking moeten staan van een team van technische experts. Dit was evenwel niet mogelijk binnen de huidige opdracht van het College.

4.2 Constatations le jour des élections

4.2.1 Contrôles dans les bureaux de votes

4.2.1.1 Bureaux contrôlés le jour des élections

Commune	Bureaux
St Josse	8 6,16,27,47,50,54,57, 63
Aalst	76
Amel	10,11,14
Anderlecht	23
Ans	23
Asse	9
Auderghem	53
Aywaille	12
Bassenge	
Berchem St-Agathe	80
Boom	7,8
Brussel	11,23
Bruxelles 1020	76,78
Bruxelles 1120	79,87,88
Burg-Reuland	19,20
Butgenbach	25,27
Dendermonde	15, 38,42
Dilbeek	6,48,69
Durbuy	4,6

Frasnes-lez-Avaing	2, 8
Ganshoren	65
Grâce Hollogne	7
Grâce Hollogne / Flémalle	50, 51
Grâce Hollogne / Flémalle Haute	26
Grimbergen	5
Halle	26
Hauset	30
Hergenrath	20
Herstal	28
Ixelles	26,27
Jette	78,81,84
Kelmis	16
Koekelberg	106
Kontich	3,5
Kraainem	8,9
Lens	1, 5, 11
Liedekerke	79
Liège	144
Lontzen	23
Mechelen	1,2,5,7
Merchtem	94,99
Molenbeek St Jean	47, 51
Raeren	29
Seraing(Bonnelles)	30
St Gilles	4,5,6,10,14
St Josse	1, 2, 6
St Vith	6,7,8
Ternat	120,122
Uccle	3, 6
Verlaine	3, 8
Villers le Bouillet (Verlaine)	7
Vilvoorde	8,9
Visé	9
Watermael	86, 88
Wezembeek-Oppem	13,14
Woluwé-St-Lambert	64
Woluwé-St-Pierre	75, 78, 88, 89,90,96,99
Zelev	11, 26
Zemst	53, 55

4.2.1.2 Constatations générales pour le système Jites

Lors de ses contrôles le Collège a souvent reçu la remarque que l'urne mettait beaucoup plus longtemps à lire la carte magnétique comparé aux élections précédentes.

4.2.1.3 Constatations générales pour le système SmartMatic

Les experts ont pu constater à de multiples endroits des erreurs de manipulation des cartes à puces pour les électeurs européens et belges résidant à l'étranger. Au lieu de choisir le type d'électeur et ensuite de faire valider la carte, plusieurs présidents ou assesseurs mettaient d'abord la carte dans le lecteur et choisissaient ensuite de le mode de l'électeur. Ceci a pour conséquence qu'un électeur européen ou belge de l'étranger recevait une carte à puce permettant de voter pour toutes les élections. Il n'est pas improbable non-plus que de ce fait, un électeur « national » ait plus tard reçu une carte pour un électeur « européen » ou « belge de l'étranger » et n'ait dès lors pas pu voter pour toutes les élections auxquelles il avait droit.

4.2.1.4 Contrôles dans les bureaux de vote

Les experts ont procédé le jour des élections à des contrôles dans de nombreux bureaux de vote. Les annexes reprennent des constatations spécifiques pour les bureaux des communes suivantes : Bruxelles, Berlare, Holsbeek, Haacht, Boortmeerbeek, Zemst, Vilvoorde, Zoutleeuw, Neerlinter, Liedekerke, Ternat, Dilbeek, Grimbergen, Brussegem, Asse, Buizingen, Eupen et Saint-Vith, Watermael-Boistfort, Auderghem, Uccle

4.2.2 Contrôle dans les bureaux de dépouillement (DEPASS - E-Counting)

Cantons / Communes	Observations
Bruxelles	<p>Des membres du Collège ont assisté aux opérations de dépouillement avec le système DEPASS pour l'élection de la Chambre pour les belges résidant à l'étranger. Les experts ont constaté que :</p> <ul style="list-style-type: none"> • Chaque bureau de dépouillement s'organise comme il veut, sous la responsabilité de son président. Il n'y a donc pas d'uniformité de fonctionnement ; • Une panne de courant est venue perturber les opérations dans un des locaux. Les experts ont assisté au redémarrage des systèmes, à l'effacement de certains bulletins encodés sur un PC et absent de l'autre de manière à ce que les deux PCs soient au même niveau d'encodage. La pile de bulletin en cours d'encodage a été parcourue pour trouver le dernier bulletin encodé et les opérations ont repris à partir du bulletin suivant.

4.2.3 Contrôle du système Web2

Geen enkele controle werd uitgevoerd in één van de 20 diplomatieke posten bij invoeren van de buitenlandse stemmen op zaterdag 24 mei.

Het college heeft na de verkiezingen 2 steekproefcontroles uitgevoerd door de data, beschikbaar in de 20 PV's opgesteld door WEB2 bij het afsluiten van de stemopnemingsbureaus, te vergelijken met de gepubliceerde resultaten op de website van FOD Binnenlandse zaken voor het speciaal kanton FOD BuZa. (type stemmen E3 en E4)

Op basis van 2 willekeurig gekozen kandidaten voor de kieskringen Luik, Luxemburg, Antwerpen, Vlaams Brabant en Henegouwen, heeft het college geen verschil gevonden voor wat betreft de voorkeursstemmen.

Voor een willekeurig uitgekozen partij heeft het college ook geen verschil gevonden voor de totalen van de stemmen voor de kieskringen Luik, Luxemburg, Antwerpen, Vlaams-Brabant, Waals-Brabant, Limburg, Oost- en West-Vlaanderen, Namen en Henegouwen.

Voor kanton Brussel kon de vergelijking niet uitgevoerd worden vanwege de toevoeging van de stemmen per briefwisseling (type E5) in kanton FOD BuZa Brussel.

Het decrypteren van de stemgegevens op de WEB2 server van FOD binnenlandse zaken gebeurde op zondag 25 mei in de cockpit van Binnenlandse zaken in aanwezigheid van een deskundige van het College. Het decryptiewachtwoord werd door de firma Stésud aangemaakt, afgedrukt, beveiligd met een afkrab strookje en door hen bewaard in een verzegelde omslag.

Deze omslag werd op de dag van de verkiezingen omstreeks 15u35 opengemaakt en de decryptieprocedure werd opgestart. De decryptie duurde ongeveer 10 minuten. De ontsleutelde gegevens werden na de

decryptieprocedure bewaard op servers bij binnenlandse zaken en door een medewerker van Stésud manueel gekopieerd om uit te printen en opgenomen te worden in de website van de verkiezingen.

Opmerking: Door Stésud werd tijdens een voorgaande vergadering met het College in de aanloop naar de verkiezingen verklaard dat de encryptie enkel kon met de decryptiesleutel en programmatorisch geblokkeerd werd om niet te kunnen opstarten voor 16u00 op de dag van de verkiezingen. **Deze programmatorische beveiliging heeft dus niet gewerkt** aangezien de werkelijke decryptie reeds om 15u35 is gestart. Ook heeft het College vragen bij de veiligheid van de procedure die gevolgd is om het decryptiewachtwoord aan te maken aangezien ze hier zelf niet bij aanwezig waren.

4.2.4 Contrôles dans les bureaux de totalisation

Les membres du Collège étaient présents dans différents bureaux de totalisation: Zele, Wetteren, Zoutleeuw, Glabbeek, Haacht, Saint-Vith, Schaerbeek, Molenbeek-Saint-Jean, Ixelles et Bruxelles. Les détails des observations sont repris dans les annexes.

4.3 Contrôles effectués après le jour des élections

4.3.1 Vérification des votes de référence

4.3.1.1 Jites

Lors de leur passage dans les bureaux de vote utilisant le système Jites, les experts ont procédé à des votes de tests. Ils ont vérifiés ces votes avec un matériel et un logiciel indépendants et propres au Collège. Tous les votes émis ont pu être reproduits et sont exacts.

4.3.1.2 SmartMatic

Lors de leur passage dans les bureaux de vote utilisant le système SmartMatic, les experts du Collège ont procédé à des votes de test qu'ils ont emportés à des fins de contrôle.

Pour vérifier le fonctionnement global du système, ils ont procédé comme suit sur un matériel SmartMatic :

- redémarrage en mode « recount » des bureaux de votes visités ;
- scan dans l'urne des votes récoltés ;
- clôture du bureau de vote.

Ils ont ensuite analysé avec un logiciel spécifique le contenu de la clé USB produite à la clôture du bureau de vote. Parallèlement, les bulletins de vote ont été dépouillés manuellement. Les résultats écrits sur la clé ont alors été comparés avec le résultat du dépouillement manuel. Les résultats se sont révélés identiques.

La même opération a été effectuée pour 6 bureaux de votes choisis au hasard.

4.3.2 Vérification des totalisations

Op 6 juni werden 2 SmartMatic urnes (willekeurig gekozen: Aalst (49) en Asse (76)) herteld, ter controle. Hiertoe werd gebruik gemaakt van een door het College ontwikkeld telsysteem.

4.3.2.1.1 Asse 76

De manuele hertelling van de urne Asse 76 heeft twee extra stembiljetten aan het licht gebracht in vergelijking met het aantal stembiljetten die de urne heeft verwerkt. Deze twee extra stemmen zijn dus de dag van de verkiezingen niet gescand geweest.

4.3.2.1.2 Aalst 49

De manuele hertelling van de urne Aalst 49 bracht eveneens de aanwezigheid van twee extra stembiljetten in de urne aan het licht.

4.3.2.1.3 Verklaring

De meest plausibele verklaringen lijken ons:

- Een kiezer die twee maal stemt (via een volmacht) heeft slechts één stem gescand en toch beide biljetten in de urne gedeponereerd. Dit ligt in de lijn met het feit dat in de urne bundels werden gevonden van 2 dichtgeplooid stembiljetten die samengeplooid waren.
- Een kiezer heeft geen groen licht gekregen ("correcte scan") en toch zijn biljet in de urne gedeponereerd.
- Referentiestemmen die in de urne terechtgekomen zijn.

Fouten, ontstaan in elk van de drie bovenstaande scenario's, zouden aan het licht moeten komen bij de "sluiting van de stemming". De door IBZ ter beschikking gestelde instructies voor de voorzitter van een SmartMatic kiesbureau (doc. met ref. QM 805/KS/2014) schrijven voor dat het aantal kiezers volgens de aanstippingslijst in het PV moet opgenomen worden in het verslag. In dit verslag moet ook het aantal geregistreerde stembiljetten worden vermeld (een getal uit het kerncijferrapport). Wij hebben een sterk vermoeden dat het voorkomt dat het aantal kiezers niet berekend wordt op basis van de aanstippingslijst, waardoor een belangrijke controle ontbreekt in de hele procedure.

In het rapport zelf wordt hier volgens ons onvoldoende de nadruk op gelegd.

Als per stembureau de gegevens op basis van de aanstippingslijsten vergeleken worden met de gegevens van het kerncijferrapport, zullen bovenstaande fouten aan het licht komen. Deze fouten kunnen dan rechtgezet worden door over te gaan tot een hertelling door het opnieuw inscannen van de stembiljetten.

4.3.2.2 Hertellen van de teststemmen uitgebracht door de leden van het college tijdens de verkiezingen

De teststemmen die tijdens de steekproeven op de dag van de verkiezingen werden meegenomen werden via een hertelling elektronisch verwerkt in een testomgeving. De elektronische resultaten van deze hertellingen werden manueel nageteld.

4.3.2.3 Recherche de bulletins de vote menant au votes de préférences de candidats

In Ham werd bij de vorige verkiezingen (in 2012) de huidige burgemeester verkozen met meer dan 1600 voorkeurstemmen. Bij de huidige verkiezingen heeft hij in de gemeente Ham slechts 42 voorkeurstemmen gehaald. De burgemeester vroeg om dit te laten onderzoeken door de FOD binnenlandse zaken.

De FOD binnenlandse zaken heeft, geconfronteerd met deze feiten, de zaak geanalyseerd (SmartMatic wordt gebruikt in het kanton Beringen) en is tot de bevinding gekomen dat er niets misgelopen is met de eigenlijke verkiezing en telling, doch dat er fouten gemaakt zijn bij het verdelen van de stemmen over de gemeenten.

De structuur van het publiceren van de resultaten blijft het kanton, doch voor statistische doeleinden worden vanaf dit jaar de resultaten ook weergegeven per gemeente.

Het kanton Beringen bestaat zo uit de gemeenten Beringen, Ham, Heusen Zolder, Leopoldsburg en Tessenderlo. Bij het weergeven van de resultaten per gemeente werden voor Ham verkeerdelijk de resultaten van andere urnen in het kanton Beringen getotaliseerd.

De stemmen die deze kandidaat niet zag verschijnen in de totalen van de gemeente Ham, kwamen aldus voor in de totalen van de andere gemeenten in het kanton Beringen.

Op een vergadering, gehouden tussen deskundigen van het College en vertegenwoordigers van de FOD BiZa, werd bovenstaande uitvoerig toegelicht.

Deskundigen van het College is, om deze stelling van de FOD te verifiëren, ter plekke geweest in het vredegericht van Beringen en heeft daar manueel het aantal voorkeurstemmen voor de kandidaat uit verschillende urnes van de gemeente Ham nageteld (meerbepaald HAM 34, HAM 35, HAM 36, HAM 37, HAM 38 en HAM 39. Ook werden de resultaten van de telling die weggeschreven werden op de USB sticks van deze urnes (en dus gebruikt zijn voor de verwerking van de stemming) door andere leden van het College gedecrypteerd. Vergelijking van deze 2 lijsten, urne per urne, heeft aangetoond dat met de gecorrigeerde lijst (waarbij de verdeling van de stemmen per kanton over de gemeenten wel correct werd doorgevoerd) de resultaten volledig in lijn liggen met de manueel getelde stemmen zelf.

Het college kan dus concluderen dat de uitleg van de FOD BiZa met betrekking tot de herverdeling van de resultaten over de gemeenten correct is. De resultaten van de stemming (die per kanton verwerkt zijn) zijn evenwel nooit (ook niet toen de herverdeling over de gemeenten nog verkeerd was) foutief geweest. De totalen over het kanton Beringen zijn dan ook nooit veranderd toen de herverdeling gecorrigeerd werd.

4.3.2.4 Recomptage d'une urne avec cartes magnétiques Hertelling van een urne met magneetkaarten

A l'occasion des analyses sur le « bug des élections 2014 », le Collège a procédé à titre d'exemple au recomptage d'une urne de Schaerbeek au moyen de son logiciel et de ses lecteurs de cartes. Cette urne devait être recomptée dans le contexte des opérations de récupération des données pour le calcul de l'impact du « bug ».

Le Collège a pu constater que les résultats du recomptage au moyen de son logiciel et de son matériel sont strictement identiques à ceux repris sur la disquette du bureau de vote en question.

Bij het analyseren van de “verkiezingsbug 2014” heeft het College als steekproef een hertelling uitgevoerd van een urne van Schaerbeek, gebruik makend van eigen software en kaartlezers. Deze urne diende herteld te worden om gegevens te kunnen recupereren om de impact van de bug te kunnen inschatten.

Het College heeft vastgesteld dat de hertelling, gebruik makend van eigen soft- en hardware, volledig dezelfde resultaten heeft opgeleverd als deze die op de diskette van het bureau voorkwamen.

4.3.2.5 Retotalisation complète pour les systèmes Jites

Une retotalisation complète a été effectuée pour les systèmes Jites dans le cadre de l'analyse du « bug des élections 2014 ». Le Collège a pu s'assurer que les résultats obtenus par sa totalisation sont identiques aux résultats repris dans les PV de bureaux de canton (voir plus bas pour les détails des opérations à propos du « bug des élections 2014 »).

4.3.2.6 Retotalisation complète d'un canton SmartMatic

Le 9 juin, le Collège a retotalisé le canton de Boom au départ des clés USB provenant des bureaux de vote. Les résultats obtenus correspondent aux résultats publiés sur le site des élections.

4.3.3 Diffusion des codes source

4.3.3.1 Code source des logiciels Jites

Le Collège a téléchargé les codes sources du système Jites mis à disposition par le SPF Intérieur sur son site Web. Le Collège a pu vérifier que ces codes sources sont identiques à ceux qu'il a reçu du SPF Intérieur.

4.3.3.2 Code source des logiciels SmartMatic

Le Collège a téléchargé les codes sources du système SmartMatic mis à disposition par le SPF Intérieur sur son site Web. Le Collège a pu vérifier que ces codes sources sont identiques à ceux qu'il a reçu du SPF Intérieur.

4.3.4 Suivi des recommandations des rapports précédents

Aanbevelingen gemaakt naar aanleiding van de verkiezing van 2012 waaraan SmartMatic gevolg gegeven heeft:

- Het probleem van de verwarring tussen de openingen voor respectievelijk kaartinvoer en papieruitvoer werd opgelost door de opening voor kaartinvoer als dusdanig te labelen.
- Het probleem dat het pictogram dat de kiezer uitnodigt om de kaart in te voeren maar daarbij niet aangeeft waar dit dient te gebeuren is door bovenstaand punt ook afdoende verholpen.
- De testmodus tijdens de opstartprocedure werd weggelaten teneinde fouten te vermijden.
- Het aantal gevallen waarin een alarm wordt gegenereerd is significant verminderd waardoor de "inflatie aan pieptonen" (rapport 2012) niet meer optreedt.
- De opstartprocedure van een kiesbureau is significant sneller en veel eenvoudiger geworden.
- Bij het opnieuw aansluiten van een USB-stick in de PC van de voorzitter (bijvoorbeeld na het opstarten van de stemcomputers) gebeurt er een synchronisatie tussen beide sticks, deze synchronisatie nam 90 seconden in beslag tijdens de verkiezingen van 2012. Hierbij werd er geen voortgang getoond aan de gebruiker waardoor deze vermoedde dat er een probleem was. Deze procedure werd verbeterd zodat de tijd tot 30 seconden beperkt blijft.
- Na het selecteren van een kieslijst is er een verplichte bevestiging onderaan rechts op het scherm nodig om de kandidaten van de lijst te zien waardoor onbedoelde keuze van een kandidaat niet langer mogelijk is.
- Er werden kleine aanpassingen gedaan om de ergonomie van het systeem te verbeteren.

Aanbevelingen waaraan geen gevolg gegeven werd:

- De print-out die uit de stemcomputer komt vermeldt nog steeds niet de naam en het nummer van het kiesbureau waarin de stem uitgebracht werd zodat een stem steeds kan getraceerd worden naar het kiesbureau.
- De verschillende types kaarten (Belgen, Belgen van het Buiteland, Europeanen) hebben allemaal hetzelfde uiterlijk, hetgeen vergissingen in de hand werkt.
- Een korte handleiding voor het digitaal stemmen werd niet in elk stemhokje teruggevonden.

5 Chronologie du "bug des élections 2014"

Cette section est consacrée à ce qui a été baptisé le "Bug des élections 2014". Les événements sont exposés dans l'ordre chronologique à partir de la détection du bug au cours de la soirée du 25 mai jusqu'au décompte final le jeudi 5 juin en fin de soirée.

5.1 Détection du bug : blocage des totalisatrices – 25 mai

5.1.1 Constat

Le dimanche 25 mai après 16h00, pendant les opérations d'importation, au niveau des cantons, des disquettes en provenance des bureaux de vote, le programme PGM3 chargé de valider et de totaliser les résultats a rejeté certaines disquettes en raison d'*incohérences entre les différents types de votes pour certaines listes*. Plus précisément, un message d'erreur indiquait – de manière un peu sibylline – que pour une liste donnée, le nombre total de cartes contenant des votes exprimés pour des candidats « Effectifs » était inférieur à la somme des cartes contenant des votes pour les catégories « Effectif seuls » et « Effectifs et suppléants », ce qui en effet semblait impossible.

Tous les cantons *Jites/Digivote* étaient concernés, à l'exception de celui de Verlaine qui ne comptait que huit bureaux, donc 8 disquettes à importer.

Le Collège d'experts a été informé du problème entre 16h30 et 17h. Certains de ses membres se sont rendus à Schaerbeek où le problème a pu être constaté *de visu*, et reproduit. D'autres experts ont constaté le même phénomène dans d'autres cantons dont ceux d'Eupen et d'Ixelles.

5.1.2 Conséquence

La poursuite des opérations dans les bureaux de totalisation de canton concernés s'est avérée impossible. Les résultats partiels (uniquement les chiffres électoraux provisoires et incomplets) ont cependant commencé à être publiés, de façon automatique, sur le site Web des élections. Cette publication n'a cependant pas été au-delà des disquettes acceptées par les totalisatrices.

5.1.3 Première explication du blocage

Durant la soirée du 25 mai, les informaticiens de la société Stésud ont tenté, en vain, de trouver une erreur au niveau du logiciel des totalisatrices. Les recherches se sont ensuite orientées vers le fonctionnement des logiciels dans les bureaux de vote, à savoir, dans un premier temps, celui des urnes et, ensuite, celui des machines à voter.

Pour analyser le contenu des votes individuels, les informaticiens de la société Stésud ont écrit un logiciel de décryptage de l'«urne électronique» sauvegardée sur les disquettes en provenance des bureaux de vote¹. L'analyse des votes individuels d'une disquette rejetée par les totalisatrices a fait apparaître que les incohérences provenaient de votes invalides pour une élection sur certaines cartes magnétiques : ces votes étaient attribués à une liste, mais ne contenaient ni un vote de case de tête, ni un vote pour un candidat effectif, ni un vote pour un candidat suppléant, ce que le logiciel de la machine à voter ne pouvait normalement pas produire. Les votes sur la même carte pour les autres scrutins restaient cependant parfaitement valides.

Le processus qui a amené au blocage est donc le suivant :

- des votes invalides sont introduits dans l'urne ;
- à la clôture du bureau de vote, la totalisation est effectuée par liste, par candidat et pour chacun des types de vote (tête de liste (catégorie 1), un ou plusieurs effectifs (catégorie 2), un ou plusieurs effectifs et un ou plusieurs suppléants (catégorie 3), un ou plusieurs suppléants (catégorie 4). Les votes invalides produisent des incohérences dans ce fichier des totaux car ils étaient ajoutés à la catégorie 3 de par l'algorithme implémenté par Stésud ;
- ces incohérences sont – correctement – détectées au niveau des totalisatrices des bureaux de canton et bloquent l'importation des résultats.

La recherche du « bug » s'est alors orientée vers une erreur dans le programme de gestion de la machine à voter.

La première conclusion a donc été que les votes de préférence avaient été perdus pour une raison encore

¹ Sur les disquettes des bureaux de vote se trouve un fichier informatique contenant une copie du contenu de chaque carte magnétique. Il s'agit d'une modification récente pour pouvoir le cas échéant supprimer les votes en cas de décès d'un candidat avant les élections. La société Stésud n'avait encore jamais exploité ce type de fichier et ne disposait pas d'un outil pour le faire.

inconnue mais que les votes de liste avaient bien été sauvés. Comme on le verra plus loin cette conclusion était partiellement erronée. C'est cependant sur cette base que le SPF Intérieur a décidé de débloquent l'importation des résultats au niveau des totalisatrices.

5.1.4 Déblocage des totalisatrices

Toujours dans la soirée du 25 mai, comme il semblait que, sur les votes invalides, les votes de liste avaient été correctement sauvés et que seuls les votes de préférence avaient été perdus, le SPF Intérieur a demandé à la firme Stésud de modifier le logiciel PGM3 en supprimant le test bloquant afin de permettre la poursuite du processus d'importation des disquettes dans les cantons concernés par le blocage.

Le fait que, pour les quelques urnes électroniques analysées, le nombre de votes invalides était très faible, a également certainement influencé cette décision.

Une procédure d'urgence, prévue dans le logiciel des bureaux de totalisation, a permis, avec l'accord des présidents des bureaux de canton, de remplacer le logiciel PGM3 par la version ainsi modifiée. Les opérations d'importation ont pu reprendre et se terminer dans tous les cantons sans rencontrer d'autre problème.

Le SPF Intérieur a décidé de continuer à publier les résultats en leur conservant leur caractère provisoire mais de ne pas publier de votes de préférence, soupçonnés d'être les seuls en cause à ce moment. Cette opération s'est déroulée entre le 25 et le 27 mai selon les cantons.

Conscient que le logiciel qui allait être ainsi utilisé sur les totalisatrices n'était pas certifié, le SPF Intérieur avait pris l'option de le faire analyser et certifier ultérieurement.

5.2 Explication du bug – 26 mai

Le lundi 26 mai au matin, une équipe d'informaticiens de la société Civadis a été appelée en renfort pour accélérer les opérations de recherche du "bug". Les sources du logiciel de la machine à voter ont été analysées et l'erreur a été détectée dans la matinée du lundi 26 mai. A partir de ce moment, le problème a pu être expliqué et reproduit systématiquement sur des machines à voter de test.

L'erreur se produit lorsque l'électeur, après avoir choisi une liste et y avoir sélectionné la case de tête et/ou un ou des candidats, se ravise en procédant comme suit :

- désélection de **toutes ses sélections** (y compris le cas échéant la case de tête) en **recliquant sur les cases sélectionnées** ;
- retour en arrière vers le choix des listes et/ou, pour l'élection du Parlement bruxellois, vers le choix de l'autre Collège communautaire ;
- choix d'une **autre liste de numéro strictement inférieur** à la liste préalablement choisie ou vote blanc; il est apparu plus tard qu'il y avait d'autres cas marginaux possibles, à savoir pour l'élection du Parlement Bruxellois, un changement de Collège électoral (passage des listes francophones aux listes néerlandophones ou inversement) ;
- poursuite du vote dans cette nouvelle liste.

Dans ce cas, le vote émis en second lieu n'est pas écrit sur la carte ; à sa place, un vote pour la première liste sélectionnée mais **ne contenant aucune sélection de candidat ni de case de tête** est enregistré sur la carte magnétique.

Le retour en arrière effectué lorsque des cases sont encore cochées dans l'écran ne produit par contre pas cette erreur.

Il est donc apparu que ces votes "incomplets" étaient attribués à une liste qui n'était pas celle choisie finalement par l'électeur.

Il est à noter que la relecture par l'électeur de la carte magnétique dans la machine à voter permettait de constater que :

- la liste sélectionnée n'était pas celle choisie par l'électeur au moment de clôturer son vote ;
- la liste sélectionnée était la liste qu'il avait choisie avant de se raviser et qu'aucun vote (ni case de tête, ni candidat effectif, ni candidat suppléant) n'avait été attribué à cette liste.

L'électeur aurait donc pu se rendre compte du dysfonctionnement en relisant sa carte. Aucun problème de ce type ne semble avoir été signalé aux présidents de bureaux de vote.

A l'issue de cette recherche, il est donc apparu que le problème se situait également au niveau du chiffre électoral des listes et non uniquement à celui des votes de préférence. En effet :

- les votes invalides ont été comptabilisés pour une liste finalement rejetée par l'électeur ;

- les votes invalides n'ont pas été comptabilisés pour la liste choisie par l'électeur; tout ce que l'on peut dire, c'est que la liste choisie par l'électeur avait un numéro inférieur à celle écrite sur la piste magnétique ;
- les votes de préférence sont, comme le vote de liste, définitivement perdus.

5.3 Premier calcul de l'impact du bug – 26 mai et 27 mai

5.3.1 Développement de deux programmes *ad hoc*

Dans la matinée du lundi 26 mai, pour connaître avec précision le nombre de votes concernés et l'impact potentiel sur les résultats des élections, le SPF Intérieur a demandé à la firme Stésud d'effectuer les opérations suivantes :

- récupérer la copie des données provenant des urnes électroniques sur les totalisatrices des bureaux de cantons², ce qui a nécessité l'accord et la présence des présidents de bureaux de canton ;
- développer un logiciel pour décrypter en masse les urnes électroniques ainsi récupérées ;
- développer un logiciel pour calculer le nombre de votes invalides et la répartition par scrutin, canton et liste.

Ce dernier point devait permettre au SPF Intérieur de calculer l'impact des erreurs en termes de répartition des sièges entre listes pour chaque scrutin et chaque circonscription électorale.

Dans la soirée du lundi 26 mai, ces logiciels ont été présentés au SPF Intérieur et audités par PwC sur la base de quelques données de test.

5.3.2 Calcul des votes invalides

Dans la soirée du lundi 26 mai et la nuit du 26 au 27 mai, ces programmes ont été utilisés pour calculer le nombre de votes invalides sur base des urnes électroniques déjà récupérées. Suite aux problèmes de lecture des disquettes et aux changements de mot de passe le jour de l'élection, il manquait encore à ce moment, plus de cent bureaux sur 1269.

Un premier tableau a été préparé par Stésud contenant le nombre de votes invalides identifiés dans 1100 bureaux (sur un total de 1269) et remis à Mme la Ministre de l'Intérieur, aux membres de son cabinet, au SPF Intérieur et au Collège d'experts. Deux types de bureaux manquaient dans ce tableau : d'une part ceux pour lesquels le jeu de disquettes avait dû être remplacé pour des raisons techniques en cours de journée et qui avaient reçu par conséquent de nouveaux mots de passe et d'autre part ceux pour lesquels l'urne électronique était illisible ou incohérente.

Ce tableau a pu être complété dans la journée du 27 par l'introduction manuelle des mots de passe pour les 138 bureaux. Pour les 31 bureaux restants (18 à Bruxelles et 13 à Liège) pour lesquels les fichiers urnes étant illisibles, la firme Stésud a utilisé le programme de dépouillement manuel PGM2 pour détecter les votes erronés. Le programme PGM2 dispose en effet d'une fonction de contrôle qui permet d'identifier des incohérences entre le chiffre électoral et le total des voix de préférence.

Il faut noter que cette dernière information n'a été transmise au Collège d'experts que le vendredi 30 mai après-midi **suite à des demandes d'explications du Collège**. Or, ce n'est pas sans importance car le programme PGM2 ne calcule le nombre de votes invalides que très indirectement et de façon marginale.

A ce stade (le 27 mai), le pourcentage de votes perdus avoisinait, selon les calculs de Stésud relayés par SPF Intérieur, les 0.06%. Cette moyenne cachait cependant des disparités entre les scrutins et les cantons, les votes erronés étant proportionnellement plus nombreux pour l'élection du Parlement Européen que pour les autres scrutins (sans doute parce que cette élection était la première proposée à l'électeur dans l'isoloir).

5.3.3 Impact sur la répartition des sièges entre les listes et entre les candidats d'une même liste après annulation des votes invalides

Un calcul a été effectué par le SPF Intérieur sur base de ces résultats incomplets.

² En effet, à la lecture des disquettes, la totalisatrice prend une copie de ces données à partir des disquettes: le fichier TABLE.URN, qui contient le total des votes, et le fichier FE_DSK.CRP, qui contient tous les votes individuels.

Ce calcul procède comme suit :

- annulation de tous les votes invalides (on sait qu'ils ont été indûment attribués) en soustrayant les votes invalides des chiffres électoraux de chaque liste impactée ;
- recalcul des quotients électoraux pour les deux listes « en concurrence ».

L'attribution des sièges est la même avant et après ce calcul.

Comme les votes invalides ne contenaient aucun vote de préférence, les résultats individuels des candidats ne sont pas à modifier.

5.3.4 Impact sur la répartition des sièges entre les listes après annulation des votes invalides et report de ces votes selon un scénario « pire des cas »

Le calcul précédent ne tient compte que de l'annulation des votes. Le Collège s'est inquiété de savoir si la répartition des sièges aurait pu être différente sans le bug.

Un calcul a été effectué par le SPF Intérieur sur base d'un scénario « pire des cas ». Ce calcul procède comme suit :

- suppression de tous les votes invalides (on sait qu'ils ont été indûment attribués) ;
- recherche de la liste la plus proche d'avoir un siège supplémentaire ;
- ajout au nombre électoral de cette liste de tous les votes indûment attribués aux listes de numéro supérieur ;
- recalcul des quotients électoraux pour les deux listes « en concurrence ».

Ce calcul montre que l'attribution des sièges n'est pas impactée par le bug, sauf dans le Parlement de la Communauté germanophone où, à une fraction de voix près (0,15 voix), si les 14 voix invalides attribuées aux listes de numéro supérieur sont attribuées au parti Vivant, ce parti obtiendrait un siège de plus au détriment de la liste CSP. En effet, le chiffre électoral de la liste Vivant passerait à 4008 (3994 + 14), avec donc un troisième quotient de 1336, alors que le même calcul pour la liste CSP donnerait un chiffre électoral de 9354 (9351 + 3), soit un 7^e quotient de 1335,85. Rappelons que ce scénario ne peut se réaliser que dans l'hypothèse où la liste VIVANT aurait reçu les 14 votes invalides et que donc la liste CSP n'aurait reçu aucun des 3 votes invalides de la liste Parti Libertarien.

5.3.5 Impact sur la répartition des sièges entre candidats d'une même liste selon un scénario « pire des cas »

En termes de voix de préférence, l'impact est impossible à évaluer car les 2250 votes réellement émis par l'électeur sont définitivement perdus. Il est donc parfaitement possible qu'en cas de proximité du nombre de voix de préférence entre candidats d'une même liste, un siège puisse passer de l'un à l'autre.

On pourrait uniquement vérifier que, pour chaque candidat non élu, si tous les votes invalides des listes de numéro supérieur à la sienne lui étaient attribués, il ne dépasserait pas, en nombre de voix de préférence, un autre candidat de sa liste ayant obtenu un siège.

A la connaissance du Collège, ce calcul n'a pas été fait de manière exhaustive par le SPF Intérieur.

Le Collège n'a pas non plus procédé à un examen exhaustif mais a néanmoins constaté que c'était bien le cas pour l'élection du Parlement de la Région de Bruxelles-Capitale. En effet, pour la liste PS de cette élection, l'attribution d'un siège se joue à 10 voix près.

5.4 Corrections proposées aux bureaux principaux des circonscriptions électorales – 27 mai

Le mardi 27 mai après-midi, les résultats obtenus, présentés à ce moment comme complets par le SPF Intérieur, ont été exposés aux différents intéressés : Mme la Ministre de l'Intérieur, certains Présidents des bureaux de circonscription et le Collège d'experts.

Ces résultats indiquaient, par scrutin et circonscription électorale, le nombre de votes “indûment” attribués à chaque liste. Le fait qu'il n'y avait pas d'impact sur la répartition des sièges entre liste a également été expliqué par le SPF Intérieur.

Il a donc été proposé aux présidents de bureaux de circonscription d'annuler les votes invalides puisqu'on pouvait affirmer qu'ils n'étaient pas destinés à la liste à laquelle ils avaient été attribués.

Les présidents des bureaux de circonscription ont accepté de présenter les explications et les corrections à apporter à leur bureau avant de procéder à la clôture officielle. Mme la Ministre a demandé la présence d'un membre du Collège d'experts lors de ces opérations de corrections qui devaient être menées à bien par un opérateur de Stésud sous le contrôle du bureau de circonscription.

Le mardi 27 à 18h, le SPF Intérieur a donné une conférence de presse à ce sujet avant de "libérer" les résultats en terme de voix de préférence.

5.5 Corrections apportées au niveau des circonscriptions électorales – du 28 mai au 30 mai

Entre le mercredi 28 mai et le vendredi 30 mai, les différents bureaux de circonscription ont, après en avoir dûment délibéré, annulé les votes invalides et clôturé leur bureaux de façon définitive. Les PV officiels sont disponibles sur le site des élections. Ceux-ci diffèrent donc de ceux des bureaux de cantons qui ont été clôturés avec les données initiales provisoires.

Le soir du mercredi 28 mai, au cours des corrections au bureau principal de Bruxelles où 4 circonscriptions électorales devaient être clôturées (deux collèges pour le Parlement européen, deux collèges pour le Parlement bruxellois), un problème est apparu.

Les contrôles du logiciel PGM2 de la totalisatrice pour le Parlement de la Région de Bruxelles-Capitale a – très logiquement – confirmé les incohérences constatées par le programme PGM3 lors de l'importation dans les bureaux de cantons. Ces incohérences étaient attendues car les contrôles de cohérence avaient été partiellement supprimés, le dimanche 25, au niveau des totalisatrices des cantons (programme PGM3 modifié).

Cependant, les incohérences au niveau des totaux ne pouvaient évidemment pas dépasser le nombre de votes invalides détectés par le programme *ad hoc* écrit à cette fin par Stésud le 26 mai et qui avait produit le tableau des corrections à incorporer. Or c'était le cas pour deux petites listes. Les explications données par Stésud dans la nuit du mercredi 28 au jeudi 29 ont finalement pu convaincre le bureau de circonscription qu'une erreur d'encodage manuel du nombre de votes invalides par Stésud en était la cause. Un nouveau tableau, cohérent cette fois avec le programme PGM2, a alors été envoyé par Stésud au SPF Intérieur qui l'a transmis au bureau de circonscription.

Le bureau de circonscription de Bruxelles a finalement annulé les votes selon le second tableau transmis et a ajouté des remarques aux PV des quatre circonscriptions concernées indiquant essentiellement que le contrôle exercé par le bureau était très marginal. Ce PV est accessible sur le site des élections : « *Le bureau principal souhaite faire observer que, en raison de nombreuses interventions "dites techniques" de tiers, il n'exerce, somme toute, qu'un contrôle très marginal sur la fiabilité des résultats. Les rectifications apportées aux résultats l'ont été sur la base des documents fournis par le programme de Stésud et par le SPF Intérieur.* » .

5.6 Rapport de la firme Stésud au Collège d'experts – 30 mai

Suite aux problèmes rencontrés à Bruxelles et dans d'autres cantons, le Collège d'experts a demandé une réunion avec le SPF Intérieur et la société Stésud le vendredi 30 mai, pour avoir des explications sur les problèmes constatés à Bruxelles. Les experts avaient également constaté des problèmes à Liège et à Eupen. En réponse à cette demande, Stésud a présenté un rapport complet au Collège d'experts en présence de représentants du SPF Intérieur et du cabinet de la Ministre de l'Intérieur.

Au cours de l'exposé de ce rapport, plusieurs éléments sont apparus :

- les tableaux de correction pour les circonscriptions électorales de Bruxelles étaient erronés ;
- le décryptage des urnes électroniques, source des calculs, était apparemment incorrect ;
- certaines urnes électroniques étaient toujours manquantes et les calculs des votes invalides dans ces urnes étaient basés sur les totaux et non sur les urnes elles-mêmes. L'exposé de Stésud parlait alors de 31 bureaux. Le SPF Intérieur a affirmé ne pas être au courant de ces 31 bureaux manquants dans le calcul transmis aux bureaux de circonscription. Le Collège a ensuite constaté qu'il s'agissait en fait de plus de 50 bureaux!

5.6.1 Les tableaux de corrections pour Bruxelles étaient incorrects

La firme Stésud a expliqué la cause du problème rencontré à Bruxelles le 28 mai : l'ordre des listes n'avait été

pas respecté, les numéros des listes ayant été confondus par Stésud avec la position de la liste sur les écrans de vote. En effet, à l'écran, les listes francophones et néerlandophones apparaissaient séparément alors que les numéros des listes étaient imbriqués. Comme, à Bruxelles, il y a, pour les scrutins européen et régional, un collège francophone et un collège néerlandophone, les nombres de votes à annuler ont été mélangés. Cette erreur ne pouvait être corrigée au niveau de la circonscription, les PV étant définitifs.

5.6.2 Le décryptage des urnes électroniques était incorrect

Certaines urnes électroniques présentaient, après décryptage, un contenu anormal, comme des caractères spéciaux, des votes mal formés ou des lignes tronquées. Stésud n'avait pas d'explication à ce phénomène. Le Collège a demandé quels contrôles d'intégrité étaient réalisés sur les urnes décryptées. La réponse fut qu'aucun contrôle n'avait été implémenté.

Le Collège a alors emporté les deux copies des urnes cryptées afin de mener ses propres analyses.

5.6.3 Des urnes électroniques étaient toujours manquantes

Selon les déclarations de Stésud, une trentaine d'urnes électroniques n'étaient toujours pas disponibles (fichiers corrompus). Le Collège a alors voulu savoir comment Stésud avait pu calculer, pour ces urnes, les votes invalides.

Il s'est avéré que, pour ces urnes, seul le fichier de totalisation était disponible. Le nombre de votes considérés comme invalides avait donc été déduit de la différence entre le chiffre électoral et la somme des votes avec voix de préférence ou case de tête. Ceci était en contradiction avec les informations préalablement transmises au Collège. Cela laissait évidemment une marge d'erreur importante que le Collège a soulignée.

5.7 Contrôles du Collège - du 31 mai au 1^{er} juin

Dans le cadre de sa mission de contrôle, le Collège a développé deux logiciels :

- un logiciel de décryptage d'urnes électroniques ;
- un logiciel d'identification et de totalisation des votes invalides.

Le Collège a également mis au point une méthode parallèle de détection des cartes contenant les votes invalides au moyen d'un logiciel public de recherche d'expressions régulières³ (méthode GREP³). Ceci permettait de trouver les cartes sans devoir les interpréter et était à utiliser en guise de contrôle exhaustif.

5.7.1 Logiciel de décryptage développé par le Collège

Au cours du week-end du 31 mai et 1^{er} juin, le Collège a construit son propre logiciel de décryptage à partir des sources publiées du logiciel des urnes. Le Collège a constaté que son logiciel donnait des résultats *a priori* plus corrects (disparition des caractères spéciaux et des votes mal formés ou tronqués). Le seul problème subsistant provenait du fait que certains fichiers urnes étaient corrompus.

Le dimanche 1^{er} juin, le Collège a prévenu Stésud et le SPF Intérieur du fait que le logiciel de décryptage de Stésud était selon toute vraisemblance "buggé". Stésud, après quelques tests, a confirmé que les résultats obtenus par le logiciel du Collège étaient corrects.

5.7.2 Logiciel d'identification et de totalisation des votes invalides

Le Collège a écrit un programme permettant d'identifier et de comptabiliser les votes invalides sur base des urnes décryptées.

Après comparaison avec les résultats présentés par Stésud, des différences sont, là aussi, apparues. Le Collège a pu confirmer, par une recherche manuelle, que le logiciel de Stésud ne détectait pas tous les votes invalides. Stésud et le SPF Intérieur ont été mis au courant de ce problème le lundi 2 juin.

5.7.3 Méthode GREP

La méthode GREP avait pour but d'identifier dans une série de fichiers décryptés les votes invalides par type

3 Du nom du logiciel GREP (Get Regular exPressions) utilisé pour cette approche.

d'élection. Cette approche était indispensable vu la complexité de l'encodage des données sur la piste magnétique à cause des 4 élections simultanées dans certaines parties du pays.

Les différents cas de figure étudiés par la méthode GREP correspondaient aux différents encodages possibles des cartes magnétiques:

- Élection du Parlement Européen (encodage identique partout)
- Élection de la Chambre à Bruxelles
- Élection de la Chambre en Wallonie
- Élection du Parlement Wallon en Wallonie sauf dans les circonscriptions d'Eupen et de Saint-Vith
- Élection du Parlement Wallon dans les circonscriptions d'Eupen et de Saint-Vith
- Élection du Parlement Bruxellois (listes francophones)
- Élection du Parlement Bruxellois (listes néerlandophones)
- Élection des membres bruxellois du Parlement Flamand.

Le logiciel GREP utilisé affichait par bureau de vote, les pistes magnétiques des cartes contenant des votes invalides.

Exemple :

7FD2N **500000**990000000 500000000100000000000000

est un vote invalide pour l'élection du Parlement Européen attribué à la liste en position 5 dans le canton d'Anderlecht, en l'occurrence le CdH .

5.8 Suite des corrections – du 2 au 5 juin

5.8.1 Communication au SPF Intérieur et à Stésud

Le lundi 2 juin, au cours d'une réunion entre les différents intervenants, le Collège d'experts a détaillé les constatations énumérées plus haut.

En conséquence, le SPF Intérieur a estimé devoir organiser :

- l'identification exhaustive des bureaux de votes dont les urnes étaient manquantes ou incorrectes,
- la récupération des disquettes de ces bureaux de vote,
- le recomptage manuel des urnes physiques lorsque les urnes électroniques se sont avérées illisibles.

5.8.2 Identification des urnes manquantes ou incorrectes

Le lundi 2 juin en fin de journée, Stésud a pu décrypter les urnes à sa disposition avec son logiciel corrigé. Les résultats ont été comparés à ceux du Collège et étaient identiques.

A la demande du Collège, des tests d'intégrité avaient été ajoutés. Ils ont fait apparaître que ce n'était pas 27 urnes, comme annoncé une semaine plus tôt, mais 57 urnes qui étaient soit manquantes soit corrompues.

5.8.3 Récolte des urnes manquantes

Les urnes manquantes ont été récupérées sur les disquettes des bureaux de vote lorsque les disquettes étaient lisibles (37 urnes). Les 20 urnes restantes ont été recomptées manuellement avec l'aide d'un opérateur de la firme Stésud et sous le contrôle des bureaux de canton concernés.

Le jeudi 5 juin au matin, la dernière urne était en possession du SPF Intérieur.

5.8.4 Décompte des votes invalides

Le jeudi 5 juin, les dernières urnes ayant été récoltées et décryptées, la détection des votes invalides a été effectuée avec le programme corrigé de Stésud.

Le Collège a procédé aux mêmes calculs avec son propre logiciel qui a – à nouveau – donné des résultats différents : le logiciel du Collège détectait des votes invalides que celui de Stésud ne détectait pas.

Finalement, après quelques ajustements, les votes invalides ont tous été identifiés le jeudi 5 juin vers 22h30.

5.9 Calcul final de l'impact des votes invalides sur la répartition des sièges entre les listes – 5 juin

Le SPF Intérieur a procédé à nouveau aux calculs d'impact sur la répartition des sièges entre listes. Les nouvelles données prises en compte pour ces calculs donnent les mêmes absences d'impacts, sauf pour le Parlement germanophone dans le scénario très particulier décrit plus haut.

Le SPF Intérieur a décidé de présenter les nouveaux chiffres définitifs aux Assemblées parlementaires pour leur permettre de valider (ou pas) leur élection en tenant compte de ces informations.

Le SPF Intérieur a transmis au Collège ses calculs sur l'impact des votes invalides sur les répartitions des sièges entre les listes. Le Collège considère ces calculs comme exacts.

5.10 Analyse du code source ayant généré le « Bug de l'élection 2014 »

Le code source des logiciels électoraux a été placé sur le site des élections. Il est donc disponible pour les citoyens qui souhaitent l'analyser. Cette section explique succinctement le « fonctionnement » du bug à travers l'analyse du code source.

Ce code est écrit en langage C.

5.10.1 Stockage des votes en mémoire

Pendant la durée d'un vote, les choix de l'électeur sont conservés dans la mémoire de la machine à voter dans 3 tableaux :

- `arcMemoScrutin` : tableau contenant une valeur par scrutin :
 - 0 indique un vote blanc
 - 1 indique un vote normal
 - 2 indique un vote « non permis » (un électeur étranger pour le scrutin Chambre par exemple).
- `arcMemoList` : tableau binaire (0 ou 1) à deux entrées : une ligne par scrutin et une colonne pour chaque liste. `arcMemoList[iScrutin][iList]` vaut 1 si la liste `iList` a été sélectionnée pour le scrutin `iScrutin` et 0 sinon.
- `arcMemoCandid` : tableau binaire à 3 entrées construit sur le même principe : une dimension pour les scrutins, une dimension pour les listes et une dimension pour les candidats. `arcMemoCandid[iScrutin][iList][iCand]` vaut 1 si le candidat numéro `iCand` de la liste `iList` a été sélectionné pour le scrutin `iScrutin`.

Pour comprendre le mécanisme du bug, il faut bien retenir que le logiciel stocke en mémoire *non pas le numéro de la liste courante, mais une table de 0 et de 1*, le 1 indiquant la liste sélectionnée. Pour un scrutin donné, `arcMemoList` ne peut évidemment contenir qu'un seul 1.

5.10.2 Sélection d'un candidat

La sélection d'un candidat est programmée dans le fichier `mod_cand.c` à la ligne 613 : lorsque l'électeur « clique » sur le candidat `_z` de la liste `_y` pour le scrutin `_x`, la fonction suivante est appelée :

```
void Cand_Select(int _x, int _y, int _z)
{
    arcMemoCandid[_x][_y][_z] = 1;
    arcMemoList[_x][_y] = 1;
    arcMemoScrutin[_x] = 1;
}
```

On voit ici qu'on stocke un 1 dans la table `arcMemoList`. Cette fonction est exécutée pour chaque candidat sélectionné.

5.10.3 Désélection d'un candidat

Lors de la désélection d'un candidat, le programme place un 0 dans le tableau des candidats (`arcMemoCandid[_x][_y][_z] = 0`) mais ne touche pas au tableau des listes `arcMemoList` qui conserve donc un 1 à la position de la liste, comme on le voit ci-dessous (extrait de `mod_cand.c`, ligne 620).

```
#ifdef EL2014
/*****
<FUNCTION>
  <NAME> Cand_Unselect </NAME>
  <TYPE> GLOBAL </TYPE>
  <DESCRIPTION>
    Specify that a selection has been undone
  </DESCRIPTION>
</FUNCTION>
*****/
void Cand_Unselect(int _x, int _y, int _z)
{
    arcMemoCandid[_x][_y][_z] = 0;
    //280613 arcMemoList[_x][_y] = 0;
    //280613 arcMemoScrutin[_x] = 0;
}
#endif /* EL2014 */
```

On peut noter que :

- cette fonction semble avoir été ajoutée pour l'élection 2014 (`#ifdef EL2014`)
- seul le candidat est annulé (`arcMemoCandid[_x][_y][_z] = 0;`)
- ni la liste ni le scrutin ne sont désélectionnés. On peut noter que deux instructions ont été d'abord ajoutées puis supprimées (elles sont restées en commentaire (`//`) dans le code). L'annulation de ces deux lignes est correcte dans la mesure où, s'il reste un candidat sélectionné, on doit garder la liste.

Malheureusement, lors de la désélection du *dernier* candidat et du retour vers l'écran de sélection des listes, le tableau `arcMemoList` n'est pas modifié et le 1 placé à la position de la liste reste donc présent.

Si plusieurs allers-retours sont opérés, plusieurs listes peuvent donc rester sélectionnées, tous les 1 restant en mémoire.

5.10.4 Ecriture sur la carte magnétique

Au moment d'écrire sur la carte magnétique, le programme boucle sur le tableau des listes et, chaque fois qu'il rencontre une valeur 1, note le numéro de la position dans une variable nommée `iList` (instruction `if(arcMemoList[i][y] == 1) iList = y + 1;`).

La boucle se poursuit jusqu'à la dernière position, même si un 1 est rencontré. Chaque valeur 1 rencontrée a pour effet d'écraser la valeur de la liste contenue dans `iList`. *C'est donc le plus haut numéro de liste ayant été sélectionné par l'électeur à un moment quelconque qui est mémorisé sur la carte.*

Le code se trouve à la ligne 281 du fichier `mod_scrut.c`.

```
int Scrut_Result(void)
{
    int iList, i, y, iDebut;

    iDebut = __C_VOTE_PLACE;

    /* Specify that a vote has been done */
    Card_Written(guszCard);

    /* For all ballots */
    for(i=0; i<giNbrScrutin; i++)
    {
        /* List's id attribution */
```