Rapport du Collège d'experts chargés du contrôle des systèmes électroniques de vote, de dépouillement et de collecte des résultats

Élections simultanées du 26 mai 2019 pour le Parlement européen, la Chambre des représentants et les Parlements de région et communauté

Bruxelles, le 7 juin 2019

Table des Matières

1 Le Collège

1.1 Composition du Collège

En application de l'article 24 de la loi du 7 février 2014 modifiée par la loi du 19 avril 2018 organisant le vote électronique avec preuve papier, les experts dont les noms suivent sont désignés pour une durée de 5 ans afin de composer le Collège permanent.

Experts désignés par la Chambre des représentants :

- effectifs : M. Bruno DE NYS, M. Karel VAN GEYT et M. Jérôme DOSSOGNE ;
- suppléants : Mme Sophie JONCKHEERE, M. Jean-Marc PAUL et M. Erwin VEREECKEN.

Experts désignés par le Parlement flamand :

- effectif : M. Bart MARTENS ;
- suppléant : M. Romain VOES.

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

- effectif : M. Emmanuel WILLEMS ;
- suppléant : M. Pascal VAN de WALLE.

Experts désignés par le Parlement de la Communauté germanophone :

- effectif : M. Daniel BRANDT ;
- suppléante : Mme Susi SARLETTE 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 de la loi du 7 février 2014, les experts effectifs ont désigné en leur sein un président, M. Emmanuel WILLEMS, et un secrétaire, M. Bart MARTENS.

1.2 Le Collège non permanent

Conformément à l'article de l'article 24 § 3 de la loi du 7 février 2014 organisant le vote électronique avec preuve papier, les experts dont les noms suivent sont désignés afin de composer le Collège non permanent à l'occasion des élections simultanées du 26 mai 2019 pour le Parlement européen, la Chambre des représentants et les Parlements de région et de communauté :

Experts désignés par la Chambre des représentants : M. Bruno PENNE et M. Pol BADOUX.

Experts désignés par le Parlement wallon : M. Jean-François DAMSEAUX et M. Alexandre BUBOIS.

Experts désignés par le Parlement flamand : M. Romeo MARYNS et M. Steven ES.

Experts désignés par le Parlement de la Région de Bruxelles-Capitale : M. Fabrice DUMORTIER et M. Jean-Michel DRICOT.

Experts désignés par le Parlement de la Communauté germanophone : M. Bruno HICK et M. Andreas SCHENK.

1.3 La mission

Le rôle, la mission et les moyens du Collège sont définis dans la loi du 7 février 2014, chapitre 7, article 25, modifié par la loi du 19 avril 2018, dont le texte suit.

« § 1. 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 ainsi que tout logiciel utilisé dans le cadre des élections même lorsque le vote se déroule selon d'autres modalités que celles prévues par la présente loi.

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 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. »

1.4 Le rapport

« § 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. »

1.5 Secret

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

1.6 Mise à disposition des moyens nécessaires

« § 4. La Chambre des représentants veille à mettre à disposition du Collège d'experts les moyens et ressources nécessaires pour l'accomplissement des tâches visées au présent article. »

2 Législation

Depuis les dernières élections simultanées de 2014, la législation organisant le vote électronique a fait l'objet de quelques modifications reprises ci-dessous.

2.1 Modifications concernant les systèmes de vote

Deux modifications ont été opérées aux systèmes de vote :

- Un système d'obturation automatique de la fente de l'urne a été ajouté afin d'éviter que l'électeur ne place son bulletin de vote dans l'urne avant de l'avoir scanné. La fente s'ouvre automatiquement après que le bulletin ait été scanné et reste ouverte pendant quelques secondes. Elle se referme ensuite pour attendre le prochain vote.
- Pour faciliter le vote des électeurs malvoyants ou aveugles, un des ordinateurs de vote présents dans les bureaux de votes des communes d'Alost et de Malines a été muni d'un boîtier électronique et d'écouteurs permettant à un électeur malvoyant ou aveugle d'exprimer son vote de manière autonome sans utilisation de l'écran de visualisation tactile.

2.2 Modifications concernant la publication des codes sources

Les codes sources sont publiés par le SPF Intérieur dans la semaine qui suit les élections. Ils ne comprennent pas les éléments de sécurité et restent accessibles pendant une période de 6 mois.

2.3 Modifications concernant le Collège d'experts

- Les membres du Collège permanent sont désignés 3 mois avant l'élection du Parlement européen. Ils restent en place tant qu'une nouvelle désignation n'a pas eu lieu.
- Le rôle du Collège d'experts est étendu à tout logiciel utilisé dans le cadre des élections, même lorsque le vote ne se déroule pas électroniquement.
- La Chambre des représentants veille à mettre à disposition du Collège d'experts permanent les moyens et ressources nécessaires à l'accomplissement de ses tâches.
- La Chambre des représentants ou un Parlement de Communauté ou de Région peuvent confier au Collège d'experts permanent des missions spécifiques de contrôle et d'étude relatives à la sécurisation et à la fiabilité des différents systèmes, logiciels et matériels utilisés lors des élections.

3 Description des systèmes

Deux systèmes sont à considérer pour le contrôle du Collège :

1. le système « Martine » développé par la société Civadis, chargé de la collecte des données de base pour l'élection (listes, candidats, intervenants, etc.), la collecte des résultats provenant des bureaux de votes ou des bureaux de dépouillement, le calcul et la diffusion des résultats des élections;
2. le système de vote électronique mis au point par la société SmartMatic et utilisé dans 157 communes de la région flamande, les 19 communes de la région de Bruxelles -Capitale et les 9 communes de la communauté germanophone.

Ces systèmes sont pour l'essentiel identiques à ceux utilisés à l'occasion des élections communales de 2018.

3.1 Description fonctionnelle globale

Avant les élections, le système Martine sert entre autres à récolter les données des candidats pour confectionner les listes. Les fichiers informatiques générés par cette opération sont intégrés à l'environnement de SmartMatic qui sert à la production des clés USB utilisées le jour des élections.

Le jour des élections, à la clôture des opérations dans le bureau de vote, la machine du président génère un fichier résultat « X7S » par élection, qui contient la totalisation des votes émis dans ce bureau.

Au bureau principal, le système Martine injecte ce fichier résultat dans un serveur central qui effectue la totalisation de tous les bureaux par commune et par canton, calcule les résultats complets de l'élection et diffuse les résultats.

Pour le vote traditionnel, dans le bureau de canton, le système Martine sert à l'encodage des résultats des bureaux de dépouillement.

3.2 SmartMatic

3.2.1 Description fonctionnelle

Le système SmartMatic existe en deux versions : la version utilisée pour la première fois en 2012 et une version 2018 utilisée dans les communes qui, à l'occasion des élections de 2018 ou de 2019, ont décidé de passer au vote électronique.

3.2.1.1 L'urne et la machine du président

La version 2012 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, tant pour la machine du président que pour les machines à voter. L'urne est composée d'un réservoir destiné à collecter les votes imprimés par les machines à voter et est coiffée d'un scanner de QR-codes.

Dans la version 2018, le PC du président du bureau de vote s'apparente à un PC à écran tactile connecté au hub USB de l'urne qui lui fournit son alimentation.

3.2.1.2 La machine à voter

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

Dans deux cantons (Alost et Malines) expérimentant une interface audio pour les mal-voyants et les aveugles, les machines à voter disposent en plus d'un boîtier permettant de brancher un casque audio et disposant de touches pour la navigation et la sélection des élections, des listes et des candidats.

À l'occasion des élections, deux versions de la machine à voter sont présentes : la version originale de 2012 et la nouvelle version de 2018. Ces deux versions diffèrent au niveau de la taille de l'appareil, des positions du lecteur de carte à puce et de l'imprimante. Pour le reste, elles offrent les mêmes fonctionnalités.

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 raccordés (clés USB, urne, valideuse de carte à puce, clavier, souris…).

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 les votes sous forme lisible ainsi que leurs représentations sous forme de QR-code.

Chaque électeur reçoit une carte à puce initialisée pour lui permettre de voter. 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. Cette carte ne sert qu'à démarrer l'opération de vote et ne contient aucune autre information ; elle ne sert pas à enregistrer le vote.

L'écran affiche des indications pendant toute l'opération de vote. Il est demandé à l'électeur de choisir la langue de l'interface. Il peut ensuite exprimer ses votes (vote

blanc, vote en tête de liste, un ou plusieurs candidats de la même liste) pour chaque élection que le système lui présente. A chaque étape, il lui est demandé de confirmer avant de passer à l'étape suivante. Lorsque l'électeur a confirmé son vote pour une élection sur l'écran tactile, le vote est définitif ; l'électeur ne peut plus le changer. 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 à main. Le contenu du QR-code est alors affiché à l'écran et l'électeur peut vérifier son vote.

L'électeur se dirige ensuite vers l'urne où il lui est demandé de placer le QR-code de son bulletin de vote au-dessus du scanner de l'urne. Après confirmation sonore et visuelle que le QR-code a bien été lu et enregistré par l'ordinateur du président, la fente de l'urne s'ouvre et l'électeur introduit son bulletin de vote dans l'urne. Il remet la carte à puce au président ou à un assesseur.

3.2.2.3 La clôture du bureau de vote

A l'issue du scrutin, le bureau de vote est clôturé et un rapport reprenant les chiffres-clés est imprimé. Ce rapport est signé de manière manuscrite par les membres du bureau de vote et joint à leur PV.

L'urne est ouverte et les bulletins « preuves papiers » sont transférés dans une enveloppe. Cette enveloppe contenant les bulletins de vote est ensuite scellée. Le procès-verbal, les clés USB du bureau et l'enveloppe contenant les bulletins de vote sont emmenés au bureau principal.

3.2.3 Éléments techniques du système SmartMatic utilisé dans les bureaux de vote

Le système SmartMatic utilisé dans les bureaux de vote s'exécute à partir des supports mémoires de type clés USB. Ces clés USB contiennent tous les programmes et toutes les données nécessaires au fonctionnement des différents ordinateurs (machine du président et machine de vote) et périphériques (urne et scanner à main présent dans un isoloir).

Les clés USB sont produites de manière centralisée et sont strictement identiques pour tous les bureaux de vote, tant pour la version 2012 que pour la version 2018 du matériel SmartMatic. Elles ne deviennent spécifiques à un bureau de vote qu'après le premier démarrage et l'introduction du nom du bureau et du mot de passe correspondant.

À partir de ce moment, les clés ne peuvent plus être utilisées que pour ce bureau de vote spécifique.

La clé contient par ailleurs deux zones de stockage, appelées « partitions » en jargon informatique : l'une est propre et spécifique aux programmes qui tournent dans le bureau de vote le jour des élections. Dans ce rapport, elle est identifiée en tant que « partition SmartMatic ». L'autre sert au stockage des données et des résultats du bureau de vote qui doivent être transférés à l'environnement Martine pour la

totalisation par commune et le calcul des résultats de cette commune. Dans ce rapport, elle est identifiée en tant que « partition Martine ».

3.2.3.1 Partition SmartMatic

À chaque bulletin de vote scanné par l'urne, une copie du vote exprimé est stockée dans un fichier signé et crypté avec extension « .VT » dans le dossier « /SAESLocal/SAES/Votes » de la clé. À la fin de la journée, ce dossier contient autant de fichiers « .VT » qu'il y a eu de bulletins scannés.

Au moment de la clôture des opérations, un fichier « résultat » avec extension «.X7S» est généré pour chaque élection. Ces fichiers sont numériquement signés et cryptés de manière à ne pouvoir être décryptés que par l'application Martine chargée de les totaliser.

3.2.3.2 Partition Martine

À la clôture du bureau de vote, les fichiers « .VT » et « .X7S », ainsi que quelques autres fichiers de contrôle, sont copiés depuis la partition SmartMatic vers la partition Martine.

Parmi les fichiers de contrôle se trouve le fichier PDF qui sert à l'impression dans le bureau de vote du «Rapport des chiffres-clés».

3.3 Martine

Martine est une plateforme en ligne multitâches, permettant, entre autres, la gestion de la structure de l'élection, du nom et du nombre des bureaux principaux, du nombre de bureaux de vote par commune et de leur adresse, des contacts, des actes de dépôts, des PV d'arrêts, des PV de dépouillement, des résultats de vote.

Les acteurs concernés par Martine sont :

- les communes,
- les bureaux principaux,
- les candidats,
- le pouvoir organisateur.

3.3.1 Infrastructure

La solution repose sur un environnement virtualisé basé sur une distribution Linux Centos/Redhat et VMware ESXi hypervisor. L'application se répartit au minimum sur 3 serveurs. Tous les modules sont déployés de manière redondante selon le principe du mode de fonctionnement « actif/actif ». Les bases de données et le filesystem serveur fonctionnent en mode « actif/passif ».

Au minimum deux lignes redondantes sont disponibles, une en production, l'autre en alerte. Les bases de données principales et de sauvegarde se synchronisent en continu. Les infrastructures sont équipées d'alimentations électriques, de connexions Internet, de switches, firewalls… redondants.

3.3.2 Logiciels

Martine est construite à partir d'ensemble de briques logicielles que l'on peut diviser en trois catégories :

- « Web modules », conçus pour les utilisateurs ;
- « Back end modules », pour gérer en arrière-plan les données et les résultats des candidats ;
- « Support modules » à usage interne pour des tâches spécifiques.

3.3.2.1 Les modules

Martine propose les modules décrits ci-dessous.

3.3.2.1.1 MA1X (Web)

MA1X offre les outils pour préparer les listes électorales.

3.3.2.1.2 MA2X (web)

MA2X est utilisée par l'équipe du bureau principal pour collecter les votes. Pour les bureaux de votes « papiers » les données sont encodées manuellement dans le système. Pour les bureaux de vote électronique, les données de vote sont obtenues via l'introduction de la clé USB SmartMatic. Les fichiers lus (fichiers ".X7S" et ".VT") sont transférés vers MA2X et enregistrés pour des traitements ultérieurs.

MA2X s'occupe également de la production des résultats partiels et définitifs par bureau principal.

3.3.2.1.3 MA3X (web)

MA3X contient les informations relatives aux bureaux de vote et aux bureaux de dépouillement : les adresses et personnes de contacts, le président et le secrétaire du bureau, etc.

MA3X est également utilisé par MA1B (voir ci-dessous) et MA2X pour autoriser l'accès des utilisateurs authentifiés.

3.3.2.1.4 MA1L

MA1L sert à la préparation des actes de dépôt des candidats.

3.3.2.1.5 MA1B (Web)

MA1B va réceptionner les actes de candidatures avant d'aboutir à un procès-verbal d'arrêt définitif avec le détail des listes reçues de MA1X. MA1B enregistre aussi les listes finalisées dans le backend Martine.

3.3.2.1.6 MA3S

MA3S supervise les opérations effectuées dans MA3X par les communes et les bureaux principaux. Les modules « Collect » et « Calcul » permettent de suivre l'arrivée des fichiers sur les serveurs centraux du pouvoir organisateur. Le module « Cockpit » permet de suivre toutes les opérations effectuées par l'ensemble des modules.

3.3.2.1.7 DECRYPT (Support)

DECRYPT offre une interface de service à MA2X afin qu'il puisse lire et renvoyer des informations à partir de fichiers de résultats de vote chiffrés. Il est défini en tant que module distinct uniquement pour la sécurité. Il n'est pas accessible à partir d'Internet et peut donc être séparé davantage au niveau du réseau pour optimiser le contrôle d'accès. Le déchiffrement nécessite la clé de déchiffrement privée pour les fichiers lus à partir de clés USB.

3.3.2.1.8 MA1-COLLECT (Backend)

MA1-COLLECT est le point d'entrée principal pour les fichiers générés, avec interface de surveillance. Il effectue une validation simple des fichiers reçus et les stocke pour un traitement ultérieur par MA2-CALCULATE. MA1-COLLECT est également utilisé par MA2X pour lire les données de résultat nécessaires à la production de ses PV finaux.

3.3.2.2 Accès aux modules

L'accès aux modules destinés aux communes, aux bureaux principaux et aux formations politiques est conditionné par l'introduction d'une carte d'identité électronique avec le code pin associé. Ces modules sont : MA3X, MA1L, MA1B, MA2X.

Les utilisateurs des modules MA3X ne sont pas connus avant l'élection par les pouvoirs organisateurs. Ils sont désignés en interne par les communes (MA3C) ou par les présidents des bureaux principaux (MA3B). Un système de SPOC (« single point of contact ») a été mis au point pour permettre l'association d'un bureau avec ses utilisateurs. Martine associe à chaque bureau principal un login/password qui est transmis aux bureaux concernés par la voie officielle mise en place par le pouvoir organisateur.

La personne qui dispose du login/password du bureau peut s'enregistrer dans MA3x en introduisant sa carte d'identité et son code pin. Cette personne devient alors le SPOC principal pour ce bureau et pourra avoir accès par la suite à ce module en utilisant uniquement sa carte d'identité. L'utilisation du login/password n'est nécessaire que pour la première connexion.

Un SPOC peut désigner un SPOC backup dans son bureau.

4 Contrôles et constatations

4.1 Contrôles effectués avant le jour des élections

4.1.1 Contrôles du système SmartMatic

4.1.1.1 Remise du code source et compilation de référence

Une réunion de remise du code source et de compilation de référence a été organisée le 27 février 2019 au SPF Intérieur en présence de l'organisme d'avis, de représentants de la firme SmartMatic et de membres du Collège d'Experts.

Prévue initialement une semaine plus tôt, la réunion avait dû être reportée. En effet, une incompatibilité entre les systèmes SmartMatic et Martine avait été découverte au niveau des modes de calcul de certains éléments de sécurité.

À l'occasion de cette réunion, SmartMatic a présenté les modifications apportées aux systèmes de vote électronique, celles-ci découlant essentiellement de recommandations des Collèges d'experts (fédéral ou régionaux) ou du CCB (Center for Cyber Security Belgium).

- activation des cartes à puces,
- présence d'un clapet de l'urne,
- mise à jour des algorithmes cryptographiques,
- mise à jour des algorithmes d'empreinte digitale (hash code),
- génération automatisée des codes d'initialisation,
- listes des caractères typographiques pouvant être utilisé dans les mots de passe,
- méthode d'introduction du mot de passe,
- police de caractère plus grande pour les noms des partis imprimés sur les billets de vote,
- gestion de l'extraction prématurée des clés USB (suite à l'incident de 2018),
- module audio et permettant la navigation et la sélections des listes et des candidats pour les électeurs mal-voyants,
- impression du rapport du bureau de vote au moyen d'une machine à voter en lieu et place d'un imprimante à jet d'encre,
- partition FAT32 pour le transferts des résultats du bureau de vote.

Certaines étaient déjà implémentées à l'occasion des élections de 2018.

L'application a ensuite été compilée sur un PC vierge. La procédure suivie fut la suivante :

- démarrage du PC de compilation sur une clé USB contenant un système d'exploitation Linux Ubuntu 14.04 LTS ;
- installation d'Ubuntu 14.04 LTS sur le PC de compilation ;
- redémarrage du PC de compilation sous Ubuntu et copie du code source fourni par SmartMatic ;
- compilation et génération de l'image disque de l'environnement ECM (machine de préparation) ;

- compilation et génération de l'image disque de la machine président (PM) et de la machine à voter (VM) ;

À la fin de la compilation, une copie du code source et des images disques générées ont été copiées sur différentes clés USB et remise sous enveloppe scellée aux représentants de l'organisme d'avis, du Collège et de SmartMatic.

Une copie a également été mise sous enveloppe scellée pour mise au coffre et une dernière copie, également sous enveloppe scellée, a été laissée au SPF Intérieur pour les étapes suivantes devant aboutir à la confection des clés USB à utiliser le jour des élections.

Enfin, des représentant du SPF Intérieur, du Collège, de l'organisme d'avis et SmartMatic se sont rendus à l'agence bancaire pour la mise au coffre.

4.1.1.2 Rapport de l'organisme d'avis

L'organe consultatif agréé pour les systèmes de vote électronique tels que décrits à l'article 4 § 3 de la loi du 7 février 2014 organisant le vote électronique avec preuve papier pour les élections du Parlement européen, de la Chambre des représentants et des Parlements de communauté et de région dans les communes où il est fait usage d'un système de vote électronique avec preuve papier est la société PricewaterhouseCoopers (PwC).

La société PwC a été mandatée pour la vérification de l'adéquation des applications du système SmartMatic (convention PwC-SmartMatic du 23 janvier 2019).

À l'occasion d'une réunion organisée le 21 mars 2019, l'organisme d'avis PWC a présenté un pré-rapport de son analyse du système de vote SmartMatic. Cette approche en plusieurs phases était indispensable afin de pouvoir tester la compatibilité entre SmartMatic et Martine au niveau des échanges de données, tous les modules de Martine n'étant pas encore terminés.

L'analyse s'est focalisée sur l'application de préparation du système de vote, y compris le système de duplication, le système du président de bureau, l'urne, les machines à voter et l'application de recomptage. PwC a réalisé de multiples contrôles automatisés et a conduit des entrevues avec l'équipe en charge du développement.

L'avis définitif a été remis le 12 avril 2019.

Les experts ont reçu copie de l'avis définitif de l'organisme d'avis le 14 avril 2019.

Cet avis mentionne toute une série de problèmes qualifiés de « non-bloquants » et pouvant être neutralisés par des procédures ou des interventions manuelles, notamment au niveau de l'application de préparation du système de vote et d'injection des listes électorales et des listes de candidats.

4.1.1.3 Inclusion d'un correctif suite à un problème détecté par le SPF intérieur avant le pré-rapport de l'organisme d'avis

Le 15 mars 2019, soit une semaine avant le pré-rapport de l'organisme d'avis, le SPF intérieur a découvert et signalé un problème au niveau des machines président de première génération. Ces machines sont équipées de souris qui n'étaient pas

reconnues par le système, SmartMatic ayant oublié de les inclure dans le fichier de configuration des périphériques pouvant être raccordés au système.

La solution au problème consistait donc à ajouter dans un fichier de configuration de la machine président, l'information permettant à celle-ci de reconnaître la souris et de l'accepter comme périphérique autorisé.

La société SmartMatic a proposé une solution technique au SPF Intérieur qui l'a soumise au Collège. Celui-ci a émis un avis négatif par rapport à la proposition faite, estimant que celle-ci et sa mise en œuvre s'écartait de manière significative et inutile de la procédure habituelle de génération de la clé USB « maître ». Il a dès lors été décidé de corriger le problème au niveau de l'image disque de la machine du président et de corriger manuellement le fichier de configuration des périphériques.

Le 25 mars 2019, en présence de représentants du SPF Intérieur, du Collège d'experts et de l'organisme d'avis, les représentants de la société SmartMatic ont corrigé l'image disque de la machine président en incluant le correctif requis au niveau du fichier de configuration des périphériques. Cette opération a été effectuée sur le PC de compilation et chaque partie a reçu une nouvelle copie de l'environnement de compilation (copie des images disque pour l'environnement de préparation, pour la machine président et pour la machine à voter).

4.1.1.4 Création de l'environnement de préparation ECM

Comme évoqué plus haut, l'environnement SmartMatic comporte un environnement de préparation de la clé USB de base dont des copies seront utilisées dans tous les bureaux de vote le jour des élections. Cet environnement de préparation comporte deux serveurs et un PC lient, tous les trois raccordés sur un réseau isolé.

L'image disque « ECM » générée lors la compilation sert à installer et configurer ce PC et ces deux serveurs.

Le 15 avril 2019, dans les locaux du SPF Intérieur, cet environnement de préparation de la clé USB de base, appelée « clé master », a été installé et démarré par les représentants du SPF Intérieur en présence de membres du Collège et de représentants de la société SmartMatic.

La liste des bureaux de votes a été chargée dans l'environnement « ECM » et les différents éléments cryptographiques nécessaires aux élections ont été générés. Le Collège en a pris une copie.

4.1.1.5 Génération des impressions d'écrans

À la suite de la clôture des candidatures enregistrées au moyen de Martine, les jeux de données contenant les listes électorales et les listes de candidats ont été chargés dans l'environnement de préparation (« ECM »).

Ceci s'est fait en présence du Collège, le 24 avril 2019.

À partir de cet environnement est alors générée une clé USB particulière qui est utilisée sur une machine à voter pour générer des captures d'écrans des listes et candidats. Ces captures d'écrans sont ensuite soumises à l'approbation des présidents des bureaux principaux.

4.1.1.6 Génération de la « clé master » pour les élections

Lors de l'approbation plus d'une centaine de corrections ont encore été demandées par les présidents des bureaux principaux pour corriger des erreurs qu'ils auraient dû détecter bien avant.

Le risque d'erreur est réel. En effet, à ce stade de préparation des élections, procéder de la sorte implique de devoir introduire deux fois toutes ces corrections, une fois dans l'environnement SmartMatic et une fois dans l'environnement Martine.

Suite à ces corrections, le pouvoir organisateur a pu générer la « clé master » et sa duplication sur plus de 9000 clés USB.

Le Collège a pris une copie de la « clé master » afin de l'utiliser comme référence pour ces contrôles après les élections.

4.1.1.7 Confection des supports mémoire

Le 10 mai 2019, le Collège a visité les locaux où les supports informatiques utilisés pour les élections ont été dupliquées. 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 copie des clés USB et de l'impression des mots de passe est du personnel propre au SPF Intérieur.

4.1.1.8 Environnement de test du Collège

Le Collège s'est doté d'un environnement de test, composé de machines virtuelles pour l'environnement « ECM » et a généré sa propre « clé master » qu'il a dupliqué à une vingtaine d'exemplaires en vue d'effectuer des tests portant sur différents cantons. Pour cela, le Collège dispose d'une machine de président et d'une machine à voter de la génération 2018 avec lesquelles il a effectué les opérations suivantes :

- ouverture d'un bureau de vote (démarrage urne et machine du président) ;
- démarrage de machines à voter ;
- émission de votes et visualisation de votes sur l'ordinateur de vote ;
- décryptage des fichiers « .VT » à l'aide d'un logiciel du Collège et comparaison avec la version lisible du vote.

Tous ces tests se sont avérés concluants sur le plan logiciel.

C'est lors de ces tests que le Collège a découvert une discordance dans les versions linguistiques du logiciel de la machine à voter. En effet, dans les versions française et allemande apparaît en fin de vote un message invitant l'électeur à vérifier son vote à l'aide du scanner à main prévu à cet effet dans un isoloir séparé. Dans la version néerlandaise, ce message n'apparait pas.

Le Collège en a averti le SPF Intérieur dès sa découverte. Celui-ci n'avait pas détecté ce problème et l'organisme d'avis non plus. Malheureusement, vu le caractère tardif de cette découverte, il n'a pas été possible d'y remédier, les clés USB ayant déjà été générées et mises sous enveloppe.

Interrogé à ce sujet, le SPF Intérieur a communiqué oralement que l'origine de ce problème se situait dans les fichiers sources fournis par SmartMatic qui s'est visiblement inspiré des fichiers de configuration utilisés à l'occasion des élections communales et provinciales en Flandre en 2018. En effet, le pouvoir organisateur de ces élections en Flandre ne souhaitait pas voir cette mention invitant le citoyen à un contrôle supplémentaire.

4.1.2 Contrôle du système Martine – module MA2X

La société PwC s'est vu confier le mandat de vérifier l'adéquation du système Martine (accord PwC-Civadis du 26 février 2019). L'analyse était limitée au module MA2X et concernait (1) la sécurité, l'intégrité, la fraude et le secret de la procédure électorale, (2) le respect de la législation, (3) le caractère fonctionnel et résilient des systèmes. PwC a effectué de nombreux contrôles automatisés et a eu des entretiens avec l'équipe de développement.

Le 17 mai 2019, le collège a assisté à la présentation du rapport de PwC sur son évaluation de MA2X (module de traitement des résultats de Martine). À ce moment-là, le Collège avait également reçu le rapport de langue française de PwC concernant MA2X.

En ce qui concerne les autres constatations, il est apparu au cours de la présentation que sur un nombre important d'entre elles, les sociétés PwC d'une part et, le fournisseur CIVADIS d'autre part, avaient de grosses divergences d'opinion sur leur interprétation correcte. Au cours de la réunion, il a été convenu d'offrir à CIVADIS la possibilité de répondre par écrit. Cette réponse serait traitée ou ajoutée au rapport d'évaluation de PwC pour arriver à une version finale.

Au moment de l'édition de son rapport, le Collège n'avait pas encore reçu ce document mis à jour.

Les commentaires suivants peuvent être formulés à propos du rapport de PwC:

- PwC n'a pas étudié un certain nombre d'aspects du système. (pages 11-12 de leur rapport). Cela inclut les systèmes utilisés dans les bureaux principaux pour lire les clés USB et / ou pour envoyer les votes comptés manuellement à la base de données centrale de Bruxelles. Comme l'expérience l'a montré, un certain nombre de ces éléments sont en effet importants pour, par exemple, la fiabilité et la convivialité du système.
- Il a été constaté que jusque peu avant les élections, des modifications avaient été apportées au logiciel (dernière version le 9 mai). Cela rend impossible une analyse approfondie du logiciel, tel que prévue dans la loi électorale.

En fin de compte, PwC a donné l'avis suivant: «Sur la base des travaux que nous avons effectués et à condition que les instructions (supplémentaires) et / ou les procédures manuelles (supplémentaires) nécessaires soient mises en œuvre et exécutées, et en vous référant à la définition de l'aptitude, les décisions prises nous avons l'assurance

raisonnable[1] - mais pas absolue - que l'application "Gestion des résultats" (MA2X) répond aux critères d'adéquation définis ci-dessus "

4.1.3 Relations entre les firmes responsables des développements

Afin de garantir l'authenticité et la fiabilité des données qui sont échangées entre les systèmes SmartMatic et Martine (développé par Civadis), données nécessaires à la création des clés USB et au calcul des résultats, différents mécanismes techniques informatiques sont mis en œuvre :

- Encryption
- Signature électronique
- Calcul d'empreinte numérique (hash code)
- Somme de contrôle (checksum)
- Etc.

La compatibilité des deux systèmes est donc indispensable et une bonne coordination entre les deux firmes responsables des développements logiciels sont essentielles. Le SPF Intérieur a informé le Collège de ce que plusieurs incidents de parcours ont émaillé la préparation des élections, les sociétés SmartMatic et Civadis (développeur de Martine) se rejetant régulièrement la responsabilité lors de problèmes de compatibilité ou d'interprétation des normes, standards et conventions à implémenter dans leurs logiciels.

Le Collège regrette vivement ce manque de collaboration entre SmartMatic et Civadis.

4.1.4 Analyse des codes sources

Le Collège d'experts a analysé succinctement, étant donné la courte durée de sa mission, la manière dont la sécurité informatique est mise en œuvre dans les différents systèmes, sur base du code source et des documents techniques reçus des entreprises. Le Collège d'experts émet dans ce rapport une série de recommandations relatives à la sécurité des systèmes de vote et à la mise en œuvre des techniques cryptographiques.

Le Collège d'experts suggère aussi des mesures (sur base de réalisations systématiques d'audits, de relectures systématiques des votes par les électeurs, de normes de qualité des codes sources et de la documentation) afin d'améliorer la transparence et la sécurité du processus électoral dans son ensemble, y compris au cours de la période précédant l'élection (développement du code source, génération et gestion des clés cryptographiques).

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

[1] En ce qui concerne le terme « certitude raisonnable » il est référé à l' Arrête royal du 26 mai 2002 relatif au système de contrôle interne au sein des services publics fédéraux (MB 31 mai 2002)

4.1.5 Analyse du CCB

4.1.5.1 Périmètre et méthodologie

Le Collège d'experts a pu rencontrer des spécialistes du Centre pour la Cybersécurité Belgique (CCB) et consulter les différents rapports rédigés par le Centre.

L'approche du CCB s'est concentrée sur plusieurs éléments :

- la gestion de la sécurité au niveau processus ;
- la sécurité du cycle de développement ;
- des recommandations et le suivi de celles-ci ;
- un exercice de pénétration du système de vote (pentesting).

En pratique, ces analyses ont été menées sous forme d'interview, en interaction constante avec les sociétés chargées de développer le système de vote (Civadis et SmartMatic), et/ou en parallèle de manière indépendante. La maturité organisationnelle des sociétés est également évaluée. Les résultats ont été présentés et classés selon, la vraisemblance du risque, sa difficulté de mise en œuvre et enfin l'impact sur les élections. De nombreuses corrections ont été demandées à Civadis et toutes les demandes ont été rencontrées.

Par rapport à l'analyse menée en 2018, un effort important a été fourni pour sensibiliser les responsables techniques des partis politiques à la cybersécurité de leurs installations (sites webs, moyens de communication) et crise.

Le CCB a également aidé à la mise en place d'un DRP (disaster recovery plan) et de procédures formelles pour les incidents envisagés.

A la suite de ces analyses et exercices, le CCB conclut que le processus peut être amélioré mais que le niveau de sécurité de l'ensemble est suffisant pour organiser les élections dans de bonnes conditions.

4.1.5.2 Cycle de développement et gestion de la sécurité

Le CCB a conduit une série d'interviews et a analysé les documents fournis par les sociétés SmartMatic et Civadis.

Globalement, le Collège d'experts constate que le CCB a identifié des vulnérabilités qui auraient pu être identifiées et corrigées par les entreprises avant de la mise en production.

4.1.5.3 Sécurité des machines à voter et de l'application de comptabilisation « Martine »

Lors de cette phase d'analyse, le CCB a procédé à des essais d'attaques du système (en mode dit « purple team »). Le CCB a relevé un certain nombre de points d'attention. Ils ont été transmis aux deux sous-traitants afin qu'ils puissent proposer des correctifs. Une réunion a ensuite eu lieu afin de passer en revue les actions qui avaient été prises.

4.1.6 Visite du Datacenter au SPF Intérieur

Les membres du Collège ont visité le centre de données de Martine le 9/5/2019. Les serveurs sont situés dans la salle des serveurs du SPF Intérieur.

Le collège a pu constater que toutes les bonnes pratiques propres aux datacenters sont appliquées :

- sécurité des personnes (accès restreints et contrôlés)
- réseaux (protégés et redondants)
- alimentation électrique (séparée et redondante)
- base de données (dupliquée en temps réel et sauvegardée sur 3 sites)

4.1.7 Participation aux séances de formation

4.1.7.1 Formations des formateurs

L'objectif était de former le personnel communal, chargé à son tour de former les présidents et secrétaires des bureaux de vote, commune par commune. Etant donné que les formations des formateurs ont eu lieu en décembre 2018 et janvier 2019 et que le Collège permanent n'en a pas été informé, le Collège n'a pas pu assister à ces formations.

4.1.7.2 Formations des présidents de bureaux de vote

Les membres du collège ont assisté aux formations des présidents et secrétaires de bureaux de vote des communes suivantes :

- Alost
- Anderlecht
- Berchem- Saint-Agathe
- Berlare
- Bruxelles
- Eupen
- Lochristi
- Liedekerke
- Lubbeek
- Saint-Josse-ten-Noode
- Saint-Vith
- Woluwe-Saint-Lambert
- Woluwe-Saint-Pierre
- Zele

Globalement, Le Collège a constaté que les formations étaient d'un excellent niveau. Quelques remarques s'imposent cependant :

- la partie clôture du bureau avec les procédures et les formulaires à remplir n'a pas été toujours été expliquée. Par conséquent beaucoup de bureaux de vote ont eu de grandes difficultés pour remplir les formulaires (Berlare, Zele) ;
- il n'y avait pas toujours de matériel de démonstration (Saint-Vith). La fourniture des machines de démonstration aurait créé des coûts qui n'ont pas été prévu dans leur budget ;

- certaines communes ont produit leur propre documentation (Berlare) ;
- certaines machines de démonstrations présentaient des problèmes (Aalst, Lochristi) ;
- il est clairement dit (et répété) que si à 7h30, le bureau n'est pas constitué, il faut lancer les PC quand même (Anderlecht, Berchem Saint Agathe , Eupen), ce qui est contraire à la législation qui demandent d'attendre que le bureau soit constitué ;
- certaines salles ne sont pas adaptées : pas de micro, pas suffisamment de bancs pour noter (Anderlecht, Berchem Saint Agathe) ;
- il est parfois conseillé de ne pas faire de publicité pour le scanner à main permettant de contrôler son vote (Bruxelles).
- Le matériel de démonstration était parfois présent mais les présidents de bureaux de vote n'étaient pas invités à le tester (Saint-Josse).
- Lors des formations il n'a pas toujours été mentionner la façon correcte de débrancher les clés USB des machines des présidents.

4.1.8 Respect des procédures

4.1.8.1 Lors de l'installation de l'environnement ECM

A l'occasion de l'installation de l'environnement ECM (cf. 4.1.1.4), le Collège a été très étonné de découvrir que certains fichiers de configuration des élections n'étaient remis au SPF Intérieur qu'à ce moment et qu'ils n'étaient pas présents dans le code source remis par SmartMatic à l'occasion de la compilation de référence. Par ailleurs, certains de ces fichiers ont par la suite dû être modifiés pour corriger quelques problèmes soulevés par le SPF Intérieur et qui n'avaient pas été détectés par l'organisme d'avis et/ou considérés comme non-bloquants.

Ces fichiers ont été soumis à l'organisme d'avis pour aval.

Le Collège déplore qu'il y ait une telle discordance au niveau des procédures entre le formalisme de la compilation de référence (avec copie en présence de témoins, mise sous enveloppes scellées, mise au coffre, etc.) et la remise de manière informelle par la société SmartMatic de certains éléments de configuration et même de programmation, qui ont une incidence sur le fonctionnement de la machine du président et le comportement de la machine à voter.

4.1.8.2 Après la clôture du dépôt des candidatures

Il a été rapporté au Collège que, bien que les listes aient été finalisées et validées par les présidents des bureaux principaux, certains ont encore constaté des erreurs dans celles-ci après leur signature formelle. Ces présidents ont alors exigé de pouvoir apporter des corrections à ces listes sans respecter la procédure imposée par la législation.

Il s'agit d'une centaine de modifications (orthographe des noms des candidats comme l'utilisation de caractères accentués ou non, noms des listes …).

À Anvers la liste 'Piratenpartij' (liste 23) manquait dans le système Martine. Le parti avait bien déposé sa liste, comme la procédure le prévoit mais elle avait été oubliée.

Un PV pour ce problème a été rédigé, et les données manquantes ont été ajoutées dans le tableau final de Martine.

Vu les limites de temps pour la confection des supports mémoire, ces exigences de dernière minute ont contraint les services du SPF INTÉRIEUR à opérer dans l'urgence ces modifications en dehors de la procédure et des dispositions légales, ce qui a pu être la cause d'erreurs.

4.2 Constatations le jour des élections

Le jour du scrutin, les membres du Collège ont procédé à des contrôles dans les bureaux de votes et dans les bureaux de totalisation.

4.2.1 Contrôles dans les bureaux de vote

Les experts ont effectué des contrôles dans un certain nombre de bureaux de vote électronique. Les contrôles ont été principalement de trois types : émission de votes de tests pour analyse ultérieure, réponse à un questionnaire-type, observation du déroulement des opérations.

4.2.1.1 Votes de test

Dans chaque bureau de vote contrôlé, des votes de test ont été émis par les experts du Collège, souvent en présence d'un assesseur désigné par le président du bureau de vote. Les votes émis ont été contrôlés dans l'isoloir prévu pour la visualisation du vote conjointement par l'assesseur et l'expert. Tous les votes ont été fidèlement reproduits à l'écran.

Les bulletins ont ensuite été emportés par l'expert pour être analysés dans un environnement propre au Collège après le jour de l'élection.

4.2.1.2 Questionnaire

Un rapport basé sur un questionnaire-type a ensuite été établi par l'expert avec la collaboration du président du bureau de vote. Les incidents éventuels y ont été consignés. Ce rapport a été établi afin de pouvoir identifier les difficultés rencontrées et de proposer des recommandations en conséquence.

4.2.1.3 Bureaux de vote contrôlés

Les bureaux de vote qui ont été contrôlés sont repris dans le tableau ci-dessous.

Canton	Commune	Bureaux de vote
Aalst	Aalst	5,6,8,61,65
Aalter	Aalter	1,4,5,14
Asse	Affligem	28,31
Saint-Vith	Amblève	11,12,13,14
Hoogstraten	Baerle-Duc	16
Zele	Berlare	18
Bilzen	Bilzen	16
Puurs-Saint-Amands	Bornem	14
Bruxelles	Bruxelles	12,13,15,25,26,28,29

Canton	Commune	Bureaux de vote
Saint-Vith	Bullange	16,17,18
Saint-Vith	Burg Reuland	19,20,21
Saint-Vith	Bütgenbach	22,23,24,25,27
Deinze	Deinze	1,3
Asse	Dilbeek-Schepdaal	45,68
Bruges	Dudzele	112
Saint-Vith	Elsenborn	22
Ixelles	Ixelles	4,13,48,51
Saint-Josse-Ten-Noode	Etterbeek	13,17,24
Eupen	Eupen	1,3,8,9,10
Lennik	Gaasbeek	4
Molenbeek-Saint-Jean	Ganshoren	55
Léau	Geetbets	12,14
Glabbeek	Glabbeek	5
Hasselt	Hasselt	8,11,57,58
Louvain	Herent	95
Molenbeek-Saint-Jean	Jette	73, 82
Kalmthout	Kalmthout	45
Eupen	Kelmis	17,18,19,20
Bruges	Knokke-Heist	182
Molenbeek-Saint-Jean	Koekelberg	104
Furnes	Coxyde	42
Courtrai	Courtrai	17,18,20,55,61
Rhode-St-Genese	Krainem	26
Lennik	Lennik-Gaasbeek	8
Louvain	Louvain	2,11,160,78,69
Léau	Linter	24
Lochristi	Lochristi	11
Eupen	Lontzen	21,23,24,25
Ostende	Ostende	64
Ixelles	Auderghem	57, 62, 77
Eupen	Raeren	27,29,30
Roulers	Roulers	42, 44
Saint-Gilles	Saint-Gilles	18
Saint-Vith	Saint-Vith	5,6,7,8
Schaerbeek	Schaerbeek	62
Anderlecht	Berchem-Sainte-Agathe	78
Molenbeek-Saint-Jean	Molenbeek-Saint-Jean	21,43
Saint-Josse-Ten-Noode	Saint-Josse-Ten-Noode	1,2,3,9,10,11,12
Saint-Josse-Ten-Noode	Woluwe-Saint-Lambert	67
Saint-Trond	Saint-Trond	17,18,20
Asse	Ternat	115
Tongres	Tongres	22
Furnes	Furnes	7
Fourons	Fourons	1
Ixelles	Watermael-Boitsfort	94,95, 96?

Canton	Commune	Bureaux de vote
Rhode-Saint-Genèse	Wemmel	45
Rhode-Saint-Genèse	Wezembeek	54
Saint-Josse-Ten-Noode	Woluwe-Saint-Pierre	99
Léau	Léau	3,9

4.2.2 Incidents dans les bureaux de vote

4.2.2.1 Procédures

4.2.2.1.1 Divers

Description

- ouverture des enveloppes des mots de passe et clés USB avant la constitution complète du bureau ;
- volet protégeant les ports USB dans les machines de vote et urne non scellé ;
- pas de contrôle des votes de test par le lecteur QR dans l'isoloir ;
- enveloppes contenant les clés USB et les codes mises dans le local de vote ;
- absence de votes de test.

Solution

Suivre les instructions du manuel.

4.2.2.1.2 Clés USB connecté à la machine du président

Description

Lors du contrôle du bureau de vote, on a constaté que les clés USB n'étaient pas connectées à l'urne, mais connectées à la machine du président.

Solution

On a éjecté correctement d'abord une clé USB et on l'a connectée à l'urne. Ensuite on a éjecté la deuxième clé USB correctement et le président a également connecté cette clé USB à l'urne.

Dans les configurations « machines président et urnes qui y sont raccordées », le Collège a vérifié que tous les ports USB sont interchangeables et n'influence pas le bon fonctionnement du système.

4.2.2.1.3 Problème de traduction spécifique pour les élections dans la Communauté germanophone

La traduction en allemand des documents « ACEG/11bis » et « Instructions pour les présidents des bureaux de vote utilisant le vote électronique avec preuve papier » ne tiennent pas compte des 4 élections dans les cantons germanophones.

Le procès-verbal en langue allemande créé par MA2X n'a pas été adapté au système de vote électronique actuelle. Il fait, par exemple, encore référence à des disquettes.

4.2.2.2 Matériels

4.2.2.2.1 Exemples

Florilège de problèmes techniques rencontrés :

- clés USB non fonctionnelles ;
- problème au démarrage de la machine du président ;
- redémarrage après clés USB en panne ;
- difficultés pour sortir des clés USB de la machine de vote ;
- mauvais fonctionnement de l'écran tactile d'une machine de vote ;
- panne de machine de vote ;
- panne de machine du président ;
- panne d'imprimante ;
- problèmes avec l'impression des preuves papier ;
- problème de lecture des preuves papier par l'urne.

4.2.2.2.2 Solution

En cas de problème avec le matériel des bureaux de vote, la société SmartMatic est contractuellement chargée de remplacer le matériel défectueux dans un délai défini selon le type de panne. Les clé USB de remplacement ont été livrés dans le délai fixé à 30 minutes pour les points qui bloquent les opérations de vote, ce qui était le cas.

4.2.2.3 Autres

4.2.2.3.1 Dysfonctionnement de l'imprimante des machines à voter et double vote

Description

Des bulletins sont restés bloqués dans l'imprimante de certaines machines à voter. Les électeurs concernés par ce problème ont pu voter à nouveau dans un autre isoloir.

Lors de l'intervention du technicien, le bulletin -- ou les bulletins attachés les uns aux autres -- ont été retrouvés à l'intérieur de la machine à voter. Ce ou ces bulletins ont été parfois erronément scannés et placés dans l'urne par un membre du bureau, enregistrant ainsi un deuxième vote pour les électeurs concernés (Saint-Gilles 18).

Solution

Il faut donner instruction aux bureaux de vote de ne jamais scanner les bulletins bloqués dans les machines à voter sans quoi cela donnerait lieu à un double vote. Ces bulletins doivent être considérés comme nuls et traités comme tels.

4.2.2.3.2 Bulletins placés dans l'urne sans avoir été scannés

Description

Il est apparu, lors de recomptages d'urne dans les bureaux principaux, que le nombre de votes scannés était supérieur à celui indiqué sur le rapport des chiffres-clés du bureau de vote. Après analyse, la seule explication plausible est que certains bulletins de vote ont été placés dans l'urne sans être scannés.

4.2.3 Contrôles dans les bureaux principaux

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

- Anvers
- Berchem Saint-Agathe

- Bruxelles
- Eupen
- Louvain
- Lennik
- Malmedy
- Saint-Gilles
- Saint-Vith
- Tongres
- Zaventem

Une majorité de PC des bureaux principaux ont connu des problèmes de connexion à l'environnement Martine (cf. 4.2.5). Le helpdesk était difficilement joignable.

Ce problème mis à part, les experts ont pu constater que certaines libertés ont été prises lors de l'acheminement des clés USB aux bureaux de cantons (enveloppes parfois non signées, parfois non scellées, parfois même sans emballage)

De même, il a dû être procédé à des recomptages d'urnes dans les bureaux principaux, avec pour seule conséquence une certaine perte de temps.

4.2.4 Incident : Publication prématurée des résultats sur les sites Web des médias

Constatation

Le jour du scrutin, vers 15 h 30, les premiers résultats (un bureau de Tongres) ont été publiés sur le site web de la VRT alors que les élections étaient encore en cours.

Des membres du Collège se sont rendus au bureau concerné où ils ont constaté que les résultats publiés étaient conformes à ceux du comptage manuel. Les discussions avec les membres du bureau de vote, et en particulier avec le président, ont permis de conclure que:

- les résultats n'avaient pas encore été saisis dans Martine ;
- le bureau de vote avait reçu la visite de journalistes.

Un responsable du SPF Intérieur a indiqué qu'aucun résultat n'avait été transmis via Martine, ce qui a été confirmé par le site Internet du SPF Intérieur où aucun résultat n'était affiché.

Il a également été établi que le système Martine n'avait pas envoyé de résultats aux medias avant 16h40.

Conclusion

La diffusion prématurée des résultats du premier bureau à Tongres a été effectuée en dehors des canaux officiels par des journalistes sur place et ne relève pas de la compétence du Collège.

La confirmation par le SPF Intérieur qu'aucun résultat n'avait été diffusé avant 16 heures (également vérifié via le serveur sftp du collège) suggère que les autres

résultats publiés par anticipation ont également été obtenus en dehors des canaux officiels.

4.2.5 Incident de la transmission des résultats à partir des cantons le soir des élections

4.2.5.1 Résumé et impact sur le résultat des élections

La procédure de vote prévoit l'envoi des résultats électroniques (contenus sur les clés USB des machines président ou encodées à la main dans le cas du vote papier) depuis les bureaux principaux vers le système Martine.

Peu de temps après l'envoi des premières données, il est apparu qu'une grande majorité des bureaux de canton n'arrivaient plus à se connecter pour s'identifier. Le système a été indisponible pendant plusieurs heures (de 16h à 20h10).

Après analyse des informations transmises au Collège, il a pu conclure que cet incident n'a pas eu d'impact sur les résultats.

4.2.5.2 Description technique des incidents sur base des informations transmises au Collège

4.2.5.2.1 Incident 1 - Accès impossible à l'environnement d'envoi des données depuis les bureaux de votes

L'incident a débuté aux alentours de 16h. Plusieurs bureaux ont téléphoné au helpdesk de Civadis pour signaler l'impossibilité de se connecter aux modules MA2X. Les modules firewall, load-balancer et bases de données continuaient à répondre correctement et les paramètres de charge étaient normaux. Cependant, il n'était pas possible d'établir de nouvelles connexions vers les systèmes. Après analyse des différents éléments (réseau et routeurs Proximus, règles de firewall, etc...), il a été constaté qu'un nombre important de sessions DNS étaient ouvertes sur le firewall de Martine. Ces sessions étaient dues au serveur DNS (privé) utilisé par les clients, et qui a été configuré pour empêcher la résolution des noms autres que ceux autorisés pour Martine. Il s'agit, selon les premières analyses, de vérifications massives de mise à jour de l'environnement Windows 7 provenant des machines mises à disposition des bureaux principaux par Civadis pour encoder et transmettre les résultats des votes, et des routeurs fournis pour l'occasion.

La décision a été prise de rediriger les requêtes DNS traitées par l'infrastructure Martine vers les serveurs DNS du SPF Intérieur. Les sessions ouvertes se sont résorbées aussitôt.

4.2.5.2.2 Incident 2 – Perte de connectivité via le réseau Publilink

Après la résolution de l'incident 1, des problèmes d'accès subsistaient. De nouvelles sessions ne pouvaient être initiées et les sessions perdues ne pouvaient être rétablies.

Après analyse, il apparait que la connectivité réseau via le réseau Publilink ne permettait pas d'atteindre correctement les serveurs de Martine alors que c'était possible depuis l'Internet ou le réseau du SPF Intérieur. Le support Martine a alors proposé le basculement de l'accès au module MA2X de Publilink vers Internet/Fedman

(sur le réseau BELNET). La solution a été validée, en terme de sécurité, par les ingénieurs du CCB et du CERT présents au SPF Intérieur.

A ce moment-là, la connectivité fut rétablie et l'envoi des résultats reprit normalement.

4.2.5.2.3 Incident 3 – filtrage bloquant sur le firewall du SPF Intérieur

En fin de soirée, un ajout de règle filtrage sur le firewall du SPF Intérieur a déconnecté les utilisateurs actifs, amenant un grand nombre d'appels au helpdesk. La règle a été supprimée et les opérations ont pu reprendre normalement.

4.2.5.2.4 Suivi des incidents et conclusion

Le lundi 27, le Collège a demandé au directeur général du SPF Intérieur une analyse complète des évènements survenus la veille, un suivi des décisions prises lors des réunions de crise et de consigner les logs des différents intervenants pour analyse ultérieure. Le SPF Intérieur a lancé une enquête interne et a pleinement collaboré avec le Collège, en totale transparence et avec rapidité.

Le Collège a pu conclure, au vu des informations qu'il a reçues et des analyses qu'il a conduites, que les problèmes informatiques n'ont provoqué que des ralentissements du processus. Les propriétés cryptographiques (intégrité des résultats de vote, authenticité des sources d'envoi dans Martine, confidentialité des communications) ont été garanties tout au long du processus. Elles sont conformes à ce qui est attendu du système de vote électronique et d'envoi des données dans Martine.

Le Collège a pu également analyser les plans de DRP (disaster recovery plan), les procédures de gestion de crise et les analyses techniques du CERT / CCB.

4.3 Contrôles effectués après le jour des élections

4.3.1 Vérification des totalisations

Comme à l'occasion des élections de 2014, et en particulier suite aux problèmes détectés lors des élections de 2018[2], le Collège a à nouveau souhaité procéder à une retotalisation complète des votes contenus dans les supports mémoires utilisés dans les bureaux de vote.

L'objectif était de comparer les résultats obtenus par le Collège au moyen de ses propres logiciels avec les données diffusées par Martine aux médias le soir des élections et également utilisées pour diffuser les résultats sur le site web officiel des élections https://elections2019.belgium.be/ .

4.3.1.1 Récupération des clés USB

Afin de pouvoir procéder à la retotalisation, le collège devait récupérer toutes les clés USB utilisées le jour des élections. À cette fin, le SPF Intérieur a envoyé une directive à tous les bureaux de canton où est utilisé le vote électronique leur demandant de

[2] Dans une commune bruxelloise et une demi-douzaine de communes flamandes, une erreur humaine de manipulation avait perturbé la clôture du système de vote, avec comme conséquence que tous les bulletins de vote n'avaient pas été comptés !

regrouper toutes les clés USB aux bureaux principaux de circonscription A (pour la Chambre) pour le lundi 27 mai avant 15h.

Malheureusement, cette directive n'a pas été lue par tous les présidents de canton. De plus, dans certains cantons, aucune procédure n'avait été mise en place pour récolter les clés USB. Il n'a pas été possible de récupérer toutes les clés. Au final, il manque 3 jeux de clés répartis sur 3 cantons différents.

4.3.1.2 Lecture des clés USB

Le Collège a mis au point un environnement informatique spécifique (système d'exploitation, logiciel) pour prendre une copie des supports mémoire utilisés dans les bureaux de vote en vue de leur analyse et de leur exploitation.

Au moyen de cet environnement, le Collège a procédé à la prise de copies de toutes les clés USB utilisées dans les bureaux principaux pour la totalisation. Il a également pris des copies des clés USB utilisées pour différents recomptages dans différentes communes. Ces recomptages avaient été décidés dans les bureaux principaux pour différentes raisons, comme le scan des votes de référence du bureau de vote ou l'annulation de bulletins de vote qui avaient été scannés mais pas encore déposés dans l'urne

4.3.1.3 Vérification et décryptage des clés USB

L'environnement de copie des supports mémoire du Collège a permis de procéder automatiquement à divers contrôles :

- comparaison des contenus des deux clés d'un même bureau ;
- comparaison des logiciels systèmes d'exploitation, logiciels exécutables et des jeux de données (communes, listes, candidats, etc.) avec ceux d'une clé USB de référence ;
- vérification et décryptage des fichiers « .VT » des clés.

Le Collège n'a constaté aucune anomalie dans les clés lisibles récupérées et est convaincu de leur authenticité. Les procédures en place, les sécurités cryptographiques en place lui permettent également de conclure qu'il s'agit bien des clés USB authentiques utilisées dans les différents bureaux de vote lors des élections.

Au moyen d'un outil logiciel reçu de SmartMatic (et dont le code source est disponible) et des différents mots de passe reçus du SPF Intérieur, le Collège a procéder au décryptage de tous les fichiers de type « .VT » en sa possession.

Le Collège a ainsi pu obtenir pour chaque bureau de vote (dont il avait au moins une clé) les fichiers « .VT » décryptés.

Étant donné les systèmes cryptographiques et de signature digitale en vigueur dans le système, ainsi que le décryptage sans erreur de tous les fichiers « .VT », le Collège est convaincu de l'authenticité des votes enregistrés sur les clés USB.

4.3.1.4 Copie des fichiers « .VT » pour les clés manquantes

Au moment de la lecture des clés USB dans le bureau de canton en vue de la collecte des résultats, le système Martine récupère également les fichiers « .VT » et les stocke sur un serveur central.

Pour pallier aux clés USB manquantes dans 3 cantons, le Collège a demandé et obtenu de Civadis, par l'intermédiaire du SPF Intérieur, une copie des fichiers « .VT » enregistrés par le système Martine le soir des élections.

Ces fichiers ont été décryptés au moyen des mots de passe correspondant au bureau de vote où ils ont été émis.

Étant donné les systèmes cryptographiques et de signature digitale en vigueur dans le système, ainsi que le décryptage sans erreur de ces fichiers « .VT », le Collège est convaincu de leur authenticité.

4.3.1.5 Retotalisation complète des clés USB par commune

Une fois les fichiers « .VT » décryptés, le Collège a utilisé un logiciel qu'il a développé pour effectuer une retotalisation complète de tous les fichiers « .VT » pour tous les bureaux de vote de toutes les communes.

4.3.1.6 Récupération des données transmises aux médias

En vue de capter les résultats publiés, le Collège s'est conformé à la procédure prévue pour les médias. Il s'agissait de mettre en place un serveur SFTP (serveur de fichiers sécurisé) sur lequel le SPF Intérieur met, via le système Martine, périodiquement les résultats intermédiaires et, dès que disponibles, les résultats finaux.

Cela a permis non seulement de saisir les résultats, mais aussi de suivre à quel moment les résultats ont été envoyés.

Les fichiers reçus ont été stockés dans une base de données locale au moyen d'un logiciel propre au Collège afin de les comparer avec les résultats obtenus après la retotalisation (voir ci-dessus).

4.3.1.7 Vérification de la retotalisation

Sur la base des totaux ainsi obtenus, le Collège a procédé à diverses vérifications tant sur les chiffres électoraux que sur les voix de préférence et les votes blancs tels que repris sur le site web officiel des élections. Il n'a découvert aucune discordance lors de ces contrôles.

De plus, pour toutes les élections, une comparaison automatisée et intégrale a été effectuée au niveau des résultats par commune, tant au niveau du chiffre électoral de chaque liste que des voix de préférence de chaque candidat et des votes en tête de liste.

Là non plus, le Collège n'a constaté aucune différence entre sa retotalisation et les données diffusées par le système Martine.

4.4 Diffusion du code source

4.4.1 Code source des logiciels SmartMatic

Le Collège a pu constater que le code source avait bien été publié sur le site du SPF Intérieur.

Le Collège a comparé ces sources avec celles reçues de SmartMatic lors de la compilation de référence pour produire les exécutables utilisés le jour des élections. Le code source publié est identique à celui obtenu de SmartMatic à l'occasion de la compilation de référence.

4.4.2 Code source du système Martine

La loi ne prévoit pas la publication du code source du système Martine.

5 Recommandations

5.1 Recommandations faisant suite au problème de transmission des résultats

[#2019-BE.1] Le Collège recommande de réviser le « disaster recovery plan » en tenant compte de manière systématique de l'impact de chaque service tiers (DNS, authentification via eID, etc.).

[#2019-BE.2] Le Collège recommande de mettre à jour les machines servant à l'envoi des données dans les bureaux principaux et d'en limiter au maximum les accès non nécessaires (p.ex. au moyen d'un firewall logiciel).

[#2019-BE.3] Le Collège recommande de mener divers tests automatisés sur l'infrastructure réelle (et non simulée) plusieurs semaines avant les élections. Ces tests devraient, entre autres, éprouver les limites de charge de l'infrastructure en conditions réelles et permettre de vérifier l'adéquation du « disaster recovery plan ».

[#2019-BE.4] Le Collège recommande de concevoir le processus comme si l'envoi des données se faisait systématiquement sur un réseau public non sécurisé.

[#2019-BE.5] Le Collège recommande d'étendre la mission de PwC de manière à inclure l'analyse des ordinateurs de transmission des bureaux de cantons.

5.2 Recommandations concernant les procédures

[#2019-BE.6] Le collège a constaté lors de ses contrôles dans les bureaux de vote que beaucoup de présidents de bureaux éprouvaient des difficultés au niveau de la procédure de fermeture du bureau (formulaires à remplir, enveloppes à utiliser, etc.) Le Collège recommande que les formations en tiennent compte et adressent ces problèmes.

[#2019-BE.7] Le Collège d'experts recommande la mise à jour du plan de gestion d'incidents avec entre autres des procédures claires encadrant les incidents qui interviendraient avant, pendant ou après le jour des élections.

[#2019-BE.8] Le Collège d'experts recommande que le contenu des clés USB soit systématiquement effacé après les élections.

[#2019-BE.9] Le Collège d'experts recommande que les procédures prévoient une identification claire, nominative et précise des personnes intervenant dans les bureaux de vote et dans les bureaux principaux lors des élections, en particulier des techniciens.

[#2019-BE.10] Le Collège d'experts recommande que la partie textuelle du bulletin de vote contienne aussi le numéro de la liste, ainsi que le nom du canton ou de la commune dans lequel le vote a été émis.

[#2019-BE.11] Le Collège d'experts recommande que les électeurs soient informés et invités à relire la version lisible et la version encodée des votes qu'ils ont exprimés avant numérisation et insertion de ceux-ci dans l'urne.

[#2019-BE.12] Le Collège d'experts recommande que les codes sources satisfassent aux exigences et critères de qualité de l'état de l'art en méthodologie de développement sécurisé de logiciels.

[#2019-BE.13] Le Collège d'experts recommande que le développement des logiciels du système de vote se fasse au moyen d'outils de développement standard, dans un code clair, lisible et pertinemment commenté et documenté. Toutes les procédures et spécifications permettant de produire les exécutables doivent être clairement décrites, être rendues disponibles et pouvoir être aisément reproduites. Tous les programmes, les librairies, leurs versions et leurs paramètres d'exécution doivent être documentés avec précision. Il s'agit d'appliquer les bonnes pratiques de développement.

[#2019-BE.14] Au vu des manquements constatés concernant le respect des procédures, le Collège d'experts recommande qu'un contrôle systématique soit effectué pour s'assurer de l'application de toutes les procédures.

[#2019-BE.15] Le Collège recommande que ses recommandations soient systématiquement lues, tout particulièrement la [#2019-BE.15].

[#2019-BE.16] Le Collège d'experts recommande de ne plus utiliser les algorithmes MD5 ou SHA-1, mais bien de passer à SHA-2 (SHA-512) ou SHA-3.

[#2019-BE.17] Le Collège d'experts recommande le nettoyage du code du système SmartMatic de manière à éviter tout code inutilisé dans le cadre des élections en Belgique.

[#2019-BE.18] Le Collège d'experts recommande que le nombre d'essais pour entrer un mot de passe soit limité et qu'une politique claire soit mise sur pied et documentée par le SPF Intérieur quant à ce qui se passe quand le nombre limite d'essais est dépassé (attente d'un délai avant de pouvoir recommencer ou bannissement).

[#2019-BE.19] Le Collège d'experts insiste pour que les résultats exhaustifs des élections soient rendus disponibles sur le site officiel des élections dans un format de données « open-data » (JSON, CSV…) afin de faciliter les contrôles.

5.3 Recommandations faisant suite aux rapports du CCB

Après lecture des rapports du CCB, les recommandations suivantes sont émises par le Collège.

[#2019-BE.20] Le Collège d'experts recommande l'amélioration du plan de crise, tant au niveau de l'infrastructure matérielle que logicielle et de le compléter par un plan de communication et/ou un « disaster recovery plan ».

[#2019-BE.21] Le Collège d'experts recommande que Martine soit développée de manière sécurisée, sans attendre que le CCB ne mène ses exercices en fin de cycle de développement.

[#2019-BE.22] Le Collège d'experts recommande de ne plus utiliser le chiffrement AES en mode CBC pour l'authentification.

[#2019-BE.23] Le Collège d'experts recommande que la documentation des systèmes soit générée et maintenue à jour pendant tout le cycle de développement et non uniquement à la fin.

[#2019-BE.24] Le Collège d'experts recommande de séparer les canaux de livraison des clefs USB et des mots de passe.

[#2019-BE.25] Le Collège d'experts recommande la mise en place d'un processus de génération des clés cryptographiques qui ne soit pas sensible au « key escrow problem » (extorsion de clés par celui qui la génère).

[#2019-BE.26] Le Collège d'experts recommande de mieux évaluer l'impact, en termes de sécurité, des interdépendances logicielles (bibliothèques externes ou open source) et des appels à des parties tierces (p.ex. pour l'authentification ou la DNS).

[#2019-BE.27] Le Collège d'experts recommande de mettre en place un système de sondes (IDS) qui permette de détecter tout trafic non désiré sur le réseau (autre que celui strictement nécessaire aux élections) et mettre en place une procédure pour nettoyer tout trafic indésirable.

[#2019-BE.28] Le Collège d'experts recommande que les systèmes utilisés dans les bureaux de canton pour la transmission de résultats soient composés d'un système d'exploitation et de logiciels libres, sécurisés et « ***hardened »,*** à l'image de ce qui se fait pour les systèmes utilisés dans les bureaux de vote.

5.4 Recommandations générales

[#2019-BE.29] Le Collège d'experts recommande que l'interface des machines à voter soit évaluée par des experts en ergonomie vis-à-vis de l'état de l'art de la discipline.

[#2019-BE.30] Le Collège d'experts recommande que chaque fichier rendu public par le pouvoir organisateur concernant les élections (résultats, code source, etc.) soit publié avec hash et signature électronique correspondante. Le Collège d'experts recommande que ces documents soient disponibles de manière permanente sur un site avec fonction de recherche.

[#2019-BE.31] Le Collège demande que la législation concernant le vote électronique soit modifiée pour que les supports mémoires (clés "USB") utilisées le jour des élections soient transmises au plus tard le lendemain des élections à 15h au Collège d'experts.

[#2019-BE.32] Le Collège insiste pour que tous les éléments de configuration et de programmation soient présents dans le code source fourni par SmartMatic lors de la compilation de référence.

6 Conclusion

Suite à la modification de la législation, le Collège est maintenant compétent pour contrôler les systèmes de vote électronique mais également *« tout logiciel utilisé dans le cadre des élections même lorsque le vote se déroule selon d'autres modalités que celles prévues par la présente loi ».* La mission du Collège est donc étendue au système informatique utilisé dans les communes et cantons utilisant le vote traditionnel « papier ».

Comme précédemment, le Collège a surtout orienté ses travaux sur les éléments que lui seul pouvait légalement contrôler, en particulier la retotalisation des supports mémoires utilisés dans les bureaux de votes électroniques. Il n'a donc pas procédé à un contrôle exhaustif des résultats de comptage et de totalisation pour le vote traditionnel, le contrôle démocratique dans les bureaux de dépouillement et dans les bureaux de cantons concernés étant assuré par les dispositions légales en vigueur.

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

- pour les communes et cantons faisant usage du vote électronique, le Collège n'a détecté aucune différence entre les résultats communiqués aux médias par le système Martine et publiés sur le site officiel des élections et la retotalisation exhaustive qu'il a faite à partir des clés USB. Le Collège en conclut par conséquent que les systèmes ont correctement récolté et totalisé les voix pour ces cantons et communes ;
- pour les communes faisant usage du vote traditionnel, le Collège n'a pas eu vent de problèmes, d'erreurs ou d'incohérences dans les résultats encodés à partir des PVs des bureaux de dépouillement et des PVs des bureaux de canton. Il considère que de tels problèmes, erreurs ou incohérences peuvent être détectés par ces bureaux eux-mêmes.

Le Collège estime donc que le problème de transmission des résultats survenu le soir des élections n'a pas eu d'impact sur les résultats de celles-ci.

Par conséquent, le Collège estime que l'objectif d'émettre les votes, de les enregistrer et de les compter selon les dispositions légales, a été atteint.

Le Collège remercie tous les intervenants avec qui il a travaillé pendant sa mission de contrôle pour leur coopération : les représentants des firmes, de l'organisme d'avis et du CCB, les membres des bureaux de vote et des bureaux principaux ainsi que le personnel des communes.

Il tient tout particulièrement à remercier les représentants du SPF Intérieur pour leur excellente collaboration, leur disponibilité et leur réelle volonté de transparence en particulier lors de l'analyse du problème de transmission des résultats.

Bruxelles, le 7 juin 2019.

Pour le Collège

Emmanuel Willems
Président

Bart Martens
Secrétaire