
Smartmatic

Avis concernant l'aptitude du prototype proposé

*Rapport
Version 1.1
21 décembre 2011*



Table des matières

1	Résumé & conclusions du management.....	4
2	Introduction.....	8
3	Délimitation et approche	9
3.1	Champ d'application de la mission.....	9
3.2	Approche de la mission	10
3.3	Base de l'évaluation technique du prototype	11
3.3.1	<i>Logiciel de référence</i>	11
3.3.2	<i>Liste des fonctionnalités de base</i>	11
3.3.3	<i>Liste de points prioritaires</i>	11
3.3.4	<i>Documents de référence</i>	12
3.4	Éléments qui sont en dehors du champ d'application du présent rapport	12

4	Évaluation technologique.....	13
4.1	Introduction	13
4.2	Cadre technologique	13
4.3	Approche et observations lors des activités de contrôle du prototype du système de vote	16
4.3.1	<i>Tests fonctionnels</i>	17
4.3.2	<i>Tests de scénario</i>	17
4.3.3	<i>Tests de volume</i>	19
4.3.4	<i>Analyse des fichiers de structure</i>	19
4.3.5	<i>Analyse du code-source</i>	21
4.3.6	<i>Vérification des spécifications du hardware</i>	22
4.3.7	<i>Évaluation des points prioritaires laissés en suspens par le passé</i>	22
4.3.8	<i>Évaluation de la documentation</i>	23
4.4	Résultat de l'évaluation technique.....	23
4.4.1	<i>Observations concernant la portée du prototype et qui sont bloquantes pour obtenir un avis « apte »</i>	24
4.4.2	<i>Observations concernant la portée du prototype et qui ne sont pas bloquantes pour obtenir un avis « apte</i>	24
4.4.3	<i>Observations qui tombent en dehors de la portée du prototype</i>	25

5	Aspects organisationnels.....	26
5.1	Temps techniques liés au prototype du système.....	26
5.2	Nombre de machines de vote nécessaires par bureau de vote	30

Annexes	33
Annexe A – Aperçu MIL.....	34
Annexe B – Rapport de Smartmatic « Tests de gros volumes » du 27 novembre 2011	35
Annexe C – Liste des points prioritaires	36
Annexe D – Liste des fonctionnalités de base.....	40
Annexe E – Rapport d'évaluation du code-source avec l'outil Sonar	45
Annexe F – Rapports d'observation détaillés (ROD)	46

NOTE IMPORTANTE

Ce document est une traduction de la version neerlandaise d.d. 21 décembre 2011. Ce document peut être utilisé à titre informatif, la version en neerlandaise étant la version valable en cas de discordances.

1 *Résumé & conclusions du management*

Historique

Le Service public fédéral Intérieur (SPF Intérieur) a publié en 2008 un Cahier des charges spécial en deux lots pour le développement d'un nouveau système de vote. En février 2011, cette mission a été attribuée à Smartmatic.

Dans ce Cahier des charges spécial, trois tâches sont prévues qui doivent être exécutées par un organisme agréé tel que prévu par l'article 2, § 2, de la loi du 11 avril 1994 organisant le vote automatisé. Ces trois tâches consistent à :

1. **Étudier la faisabilité** de l'application proposée qui sera finalement mise en œuvre pendant les élections automatisées sur le plan technologique, organisationnel, juridique et écologique, sur la base d'un prototype et de la documentation mise à disposition ;
2. Vérifier l'aptitude de ce **prototype** (cf. le Cahier des charges spécial Lot 1 Poste 1) ; et
3. Vérifier l'aptitude de **l'application** qui sera mise en œuvre pendant les élections (cf. le Cahier des charges spécial Lot 2 Poste 1).

Pour notre avis concernant la faisabilité de l'application proposée (cf. point 1), nous renvoyons à notre rapport : « Avis concernant la faisabilité de l'application proposée pour le vote électronique et l'aptitude du prototype proposé, version 1.1 du 12 juillet 2011 » et à notre rapport du 20 octobre dernier.

Ce rapport traite des questions autour de l'aptitude du prototype (cf. point 2) et de l'aptitude de l'application qui sera mise en œuvre pendant les élections (cf. point 3). Cette dernière n'a été examinée que dans le cadre de la portée du prototype.

Portée du prototype et de l'application

Dans le cadre de l'évaluation, nous avons défini le prototype comme étant une application qui comporte les fonctions *de base*¹ de l'application proposée. Le Cahier des charges spécial mentionne dans la section D.A.1. « Le développement d'un prototype de système de vote électronique dont vous trouverez *une description non exhaustive* jointe ci-après à titre informatif (...) ». Le cahier des charges fait donc implicitement une distinction entre d'une part les fonctions de base, en d'autres mots le prototype (Lot 1 Poste 1) et d'autre part toutes les autres fonctions, sans en donner de liste exhaustive, en d'autres mots l'application (Lot 2 Poste 1).

Vu que l'énumération non exhaustive des fonctions de base a donné lieu dans le passé à des interprétations différentes de la notion de prototype, celles-ci ont été énumérées de manière exhaustive avant le début de l'évaluation et validées par le développeur Smartmatic et les représentants des pouvoirs participants. Cette liste exhaustive est reprise en annexe D.

¹ Page 9 du Cahier des charges : « Le hardware du système de vote électronique doit pouvoir faire l'objet de démonstration de fonctionnalités de base telles que définies en D.A.1. ».

Pendant le parcours de développement, le pouvoir adjudicateur a été confronté à plusieurs points laissés en suspens ('issues') qui devaient être clarifiés ou résolus. Ces 'issues' ont été consolidés dans une liste ('Master Issue List' ou MIL, cf. Annexe A). En préparant la certification de la nouvelle version du prototype du système, le groupe de travail et le Groupe d'accompagnement ont fixé des priorités, ce qui a conduit à établir une liste des points prioritaires qui devaient être résolus dans le prototype du système. Pour chacun des points prioritaires, des critères d'acceptation ont été définis entre Smartmatic et les pouvoirs publics. Vous trouverez en Annexe C la liste définitive des points prioritaires telle que définie au cours de la réunion du groupe de travail du 24 novembre 2011.

Le prototype du système doit donc, outre les fonctionnalités de base, offrir également une solution à ces points prioritaires. Tous les autres problèmes connus, repris dans la MIL, qui n'ont pas été désignés comme prioritaires ont été considérés comme n'étant pas nécessaires pour le prototype du système et tombent dès lors en dehors de la portée du présent rapport

Dans le cadre de la présente évaluation, la portée de l'application (cf. Le Cahier des charges spécial Lot 2 Poste 1) est assimilée à la portée du prototype (Cahier des charges spécial Lot 1 Poste 1) ; autrement dit, l'application doit répondre aux fonctionnalités de base exigées et aux points prioritaires. Lorsque, dans ce rapport, il est fait référence au prototype, ceci doit être considéré comme étant le prototype ainsi que l'application, en tenant compte cependant de la portée définie.

Systemes qui entrent dans le champ d'application de l'évaluation

Au départ de l'évaluation de l'aptitude du prototype, les systèmes suivants² entrent dans le cadre de la mission :

- **L'application de préparation** pour préparer un outil pour démarrer les bureaux de vote ;
- **Le système du président** ;
- **Le système de vote** lui-même pour l'expression du vote par un électeur ainsi que la vérification du vote émis ;
- **Le système d'enregistrement** pour enregistrer tous les votes émis de manière électronique ; et
- **Le système de totalisation** pour totaliser les résultats de plusieurs bureaux de vote.

Aspects qui n'entrent pas dans le champ d'application de l'évaluation

Tous les autres systèmes que ceux précisés ci-dessus qui sont utilisés pour l'organisation des élections (par exemple, l'**application des candidats**, les applications pour le calcul de la **répartition des sièges** et pour la **publication** des résultats) et les interfaces relatives à ces applications tombent explicitement en dehors du champ d'application de cette mission. L'exportation de l'application proposée vers le format de l'application existante de répartition des sièges (format CODI) a cependant bien été prise en compte.

Les modifications, effectuées ou projetées, sur le hardware, les données de tests, le logiciel et la documentation après le 30 novembre 2011 tombent explicitement hors du cadre de cette évaluation.

² Une « version » ou un « système » est une combinaison de hardware, de données de test, de software, de données de configuration et de documentation

Aucun test technique n'a été effectué et l'évaluation des circonstances physiques (température, humidité, etc.) dans lesquelles les systèmes de vote automatisé seront utilisés tombe également en dehors du champ d'application de la présente étude.

Versions évaluées

La version évaluée³ est celle qui a été mise à notre disposition le 30 novembre 2011 par Smartmatic.

Évaluations effectuées

Pour vérifier l'aptitude de ces systèmes, nous avons évalué ceci :

- par rapport en premier lieu à la liste exhaustive des fonctionnalités de base et des points prioritaires (issues³), et par rapport au Cahier des charges, à l'offre de Smartmatic, à la Note conceptuelle, aux 16 modifications formellement demandées (change requests), à l'étude du Consortium des Universités « BeVoting – Étude des systèmes de vote automatisé », aux 112 recommandations du Conseil de l'Europe, aux lois électorales et linguistiques pertinentes, aux décrets et à la réglementation (en vigueur aujourd'hui) ;
- en effectuant différents types de tests qui englobent la chaîne complète du processus électoral qui tombe dans le champ d'application de la présente mission. Ces tests comprennent notamment des tests de scénario, des tests de régression, l'analyse du code-source au moyen de l'application Sonar et des fichiers de structure et la vérification de la compatibilité du logiciel avec le hardware.

Vu (a) les tests de volume menés précédemment par PwC (cf. Le rapport de PwC du 20 octobre 2011), (b) l'expérience pilote à grande échelle du 27 octobre 2011, où plus de 6.000 citoyens ont testé le système de vote électronique et (c) les tests de volume complémentaires menés par SMMT après l'expérience pilote, où 30.000 votes ont été émis, répartis sur 9 configurations de test (cf. le rapport de Smartmatic « Tests de gros volumes » du 27 novembre 2011, lesquels sont repris en Annexe B), il n'a pas été effectué de tests supplémentaires dans le cadre de nos activités de contrôle pour la certification du prototype.

Les problèmes détectés pendant l'évaluation ont été intégrés dans la Master Issue List. Les points laissés en suspens (« MIL issues ») en date du 21 décembre ont été consolidés dans des observations. Ces observations ont été réparties dans les trois catégories suivantes :

1. Observations concernant la portée du prototype et qui sont **bloquantes** pour obtenir un avis « apte » (0 observations) ;
2. Observations concernant la portée du prototype, mais qui **ne sont pas bloquantes** pour obtenir un avis « apte » (10 observations) :
 - La redondance de données sur la clef USB 'Master' concernant les fichiers election.xml peut encore être diminuée, afin de gagner du temps pendant le processus de préparation (ROD-001).
 - Il n'y a pas de fichiers PDF des écrans de dialogue créés pendant la création des écrans sur l'application ECM (ROD-002).

³ Une « version » ou un « système » est une combinaison de hardware, de données de test, de software, de données de configuration et de documentation.

- Il n'y a pas de "log" convivial présent des modifications apportées via la fonctionnalité "change candidate names" (ROD-003).
- Les tests de diagnostic ne sont pas tout à fait conformes aux critères d'acceptation (ROD-004).
- L'application RTS n'est pas toujours stable dans un usage normal (ROD-005).
- Lorsqu'on retire la clef USB master, cela ne s'indique pas sur les PC 'esclaves' du même réseau (ROD-006).
- Il n'y a pas de confirmation obligatoire de la date et de l'heure après s'être connecté dans l'application RTS (ROD-007).
- Les procès-verbaux et les fichiers de résultats exportés au niveau de la totalisation contiennent encore des erreurs (ROD-008).
- Le hardware a présenté parfois un comportement instable pendant l'exécution des plans de test (ROD-009).
- L'usage de la carte e-ID pour signer les procès-verbaux au niveau de la totalisation n'est pas conforme à la politique des cartes e-ID (ROD-010).

3. Observations qui tombent en dehors de la portée du prototype.

Un aperçu des observations laissées en suspens et le lien avec les problèmes sous-jacents sont repris dans le Chapitre 4.4 'Résultats de l'évaluation technique'. La Master Issue List avec les points détaillés est reprise en Annexe A.

Avis

Sur la base des activités effectuées par nous, nous pouvons affirmer avec une certitude raisonnable⁴ que :

- le **logiciel est compatible avec le hardware mis à disposition** ; et
- pour la portée définie, le **prototype** (cf. Cahier des charges spécial Lot 1 Poste 1) et l'**application** (cf. Cahier des charges spécial Lot 2 Poste 1) **sont aptes**.

Cet avis est exclusivement destiné à l'usage du SPF Intérieur et des autorités concernées dans le cadre du Cahier des charges spécial.

Veuillez agréer, l'expression de notre plus haute considération.

Floris Ampe
Associé
PwC

⁴ Pour les termes « certitude raisonnable », nous renvoyons à l'Arrêté Royal du 26 mai 2002 relatif au système de Contrôle interne au sein des services publics fédéraux (publié le 31 mai 2002).

2 Introduction

Le Service public fédéral Intérieur (SPF Intérieur) a publié en 2008 un Cahier des charges spécial pour le développement d'un nouveau système de vote. En février 2011, ce marché a été attribué à Smartmatic.

Dans le Cahier des charges spécial, trois tâches sont prévues qui doivent être exécutées par un organisme agréé par le SPF Intérieur. Smartmatic a choisi PwC, un organisme agréé par le gouvernement fédéral en matière de logiciel de vote, pour effectuer ces trois tâches. Ces trois tâches consistent à :

- étudier la faisabilité de l'application proposée qui sera finalement mise en œuvre pendant le vote automatisé sur le plan technologique, organisationnel, juridique et écologique, sur la base d'un prototype et de la documentation mis à disposition ;
- vérifier l'aptitude de ce prototype ; et
- vérifier l'aptitude de l'application qui sera mise en œuvre pendant les élections.

Pour l'étude de faisabilité, nous vous renvoyons à notre rapport « Avis concernant la faisabilité de l'application proposée pour le vote électronique et l'aptitude du prototype proposé, version 1.1 du 12 juillet 2011 » et à notre rapport « Avis concernant l'aptitude du prototype et du système de vote proposé et mise à jour de l'avis concernant la faisabilité de l'application proposée pour le vote électronique, version 1.0 du 20 octobre 2011 ».

Le présent rapport concerne l'évaluation du prototype tel qu'il était mis à la disposition de PwC le 30 novembre 2011. Ce prototype de système de vote consiste tant en hardwares qu'en logiciels, données de test, documentation et éléments de configuration pour supporter les processus suivants :

- tous les éléments relatifs à la préparation des élections (procédures de génération) ;
- la gestion des bureaux de vote et de l'enregistrement des votes émis ; et
- la totalisation des votes au niveau requis par type d'élection.

Le chapitre suivant traite du champ d'application et de l'approche des activités de contrôle. Le chapitre 4 contient notre évaluation technique du système proposé. Le cinquième et dernier chapitre traite de deux aspects organisationnels spécifiques, à savoir d'une part le temps (technique) nécessaire pour réaliser le processus de préparation et pour ouvrir les bureaux de vote et d'autre part le nombre minimum de machines de vote nécessaires dans un bureau de vote pour le traitement de 2.000 électeurs dans le laps de temps d'ouverture du bureau de vote (de 8 h. à 15 h.).

Les résultats et conclusions de nos activités doivent permettre aux pouvoirs publics concernés de décider en connaissance de cause de l'aptitude du système proposé.

3 *Délimitation et approche*

3.1 *Champ d'application de la mission*

Le prototype développé par Smartmatic devait, selon le Cahier des charges spécial, consister dans les éléments suivants qui font tous partie de notre mission :

- Le logiciel de préparation pour générer un médium qui sera utilisé pour sécuriser tous les bureaux et leur permettre de démarrer isolément ;
- Le logiciel d'équipement du président qui devra servir à ouvrir et clôturer le bureau de vote ;
- Le système de vote lui-même pour que l'électeur puisse émettre son vote ainsi que vérifier son vote émis ;
- Le logiciel d'enregistrement pour enregistrer tous les votes émis de manière électronique ; et
- Le logiciel de totalisation qui totalisera les résultats de plusieurs bureaux de vote au niveau du canton et de la commune et transmettra les données à un ordinateur central.

Le Cahier des charges spécial exige que les activités de contrôle soient menées dans les trois régions du pays en Belgique. Le SPF Intérieur a cependant confirmé que la Région wallonne ne devait pas être reprise dans cette évaluation en ce qui concerne l'organisation des élections locales (c'est-à-dire provinciales et communales). Par conséquent, l'impact de l'introduction de ce prototype n'a pas été évalué pour l'organisation des élections locales en Wallonie.

Dans le cadre de notre mission, il est également important de préciser que dans la plateforme électorale end-to-end actuelle, le système de vote n'est qu'un maillon d'une chaîne plus large. Cette chaîne peut être schématisée comme suit :



Plus précisément, pour la gestion des candidats, on recourt à une application spécifique. L'output de cette application, ce qu'on appelle les fichiers CODI, qui constitue logiquement un input pour le système de vote, est rendu disponible dans une forme de fichier spécifique, à savoir le 'Format F'. L'output du système de totalisation, à savoir le résultat consolidé du flux des urnes, doit par contre former un input utilisable pour une application indépendante qui est utilisée pour calculer la répartition des sièges.

Le Cahier des charges spécial prévoit qu'un organisme de conseil agréé doit contrôler aussi bien le logiciel que sa compatibilité avec le hardware. Tous les logiciels et hardwares autres que ceux décrits ci-dessus au point 3.1 (à savoir l'application des candidats, les systèmes pour le calcul de la répartition des sièges et pour la publication des résultats) qui sont utilisés pour l'organisation des élections tombent explicitement en dehors du champ d'application de notre mission.

PwC ne s'exprime pas explicitement sur l'intégration du système, qui fait l'objet de cette évaluation, avec d'autres systèmes utilisés pour l'organisation des élections et l'exploitation des systèmes le jour des élections. Cependant, vu l'exigence que le système doit être à même de mettre en mémoire les fichiers CODI, nous avons accordé une attention spécifique à ce point et l'avons repris dans notre évaluation. Pour la validation concrète, nous avons utilisé des fichiers CODI qui ont été mis à notre disposition par le fournisseur.

Enfin aucun test technique n'a été effectué et l'évaluation des circonstances physiques (température, humidité, etc.) dans lesquelles les systèmes de vote automatisé seront utilisés tombe également en dehors du champ d'application de la présente étude.

3.2 Approche de la mission

Nous schématisons ci-après notre approche générale lors de la réalisation de nos activités de contrôle du prototype de système de vote. Nous y distinguons les activités suivantes :



Les cinq premières activités ont déjà été menées dans le cadre de l'étude de faisabilité et de nos activités précédentes de contrôle sur le prototype du système (cf. notre rapport « Avis concernant la faisabilité de l'application proposée pour le vote électronique et l'aptitude du prototype proposé, version 1.1 du 12 juillet 2011 ») et notre rapport « Avis concernant l'aptitude du prototype et du système de vote proposé et mise à jour de l'avis concernant la faisabilité de l'application proposée pour le vote électronique, version 1.0 du 20 octobre 2011 ». Le résultat de ces activités a servi de base pour notre évaluation de la nouvelle version du prototype du système. Chacune des activités précitées est détaillée ci-après.

Acquisition de la connaissance

Dans cette étape, il est pris connaissance de la solution proposée par le constructeur du système pour le prototype de système de vote électronique. Cela se déroule sur la base de son offre introduite pour le Cahier des charges spécial RRN 3/2008 et d'autres documentations mises à disposition (cf. 3.3.4 Documents de référence).

Identification des risques

Au moyen d'une analyse des risques, sont analysées la possibilité et les conséquences de l'introduction du prototype proposé à grande échelle. Dans cette étape, une liste est dressée des risques auxquels un système de vote électronique est exposé.

Définition du contrôle des objectifs

Après l'identification des risques, les objectifs de contrôle en sont déduits. Un objectif de contrôle est une description du résultat souhaité ou du but à atteindre par la mise en place de contrôles. Ce sont les exigences minimales pour la gestion efficace d'un processus spécifique et des risques qu'il contient. Un exemple d'objectif de contrôle : « Le logiciel de vote est-il à même d'enregistrer tous les résultats du vote de manière complète et appropriée sur le médium prévu à cet effet ? ».

Déterminer et documenter les contrôles clefs

Dans cette étape, il est examiné quels sont les contrôles efficaces requis pour atteindre les objectifs du contrôle. Les contrôles essentiels ou contrôles clefs y sont choisis et documentés. Un contrôle concret pourrait être par exemple : « L'application sur la machine du président n'enregistre pas le résultat du vote des bulletins de vote qui ne sont pas remplis dans le bureau de vote pertinent. »

Exécuter un « desktop research »

Dans les exigences pour l'étude de faisabilité et le contrôle du prototype, il est fait référence à la faisabilité pratique des aspects organisationnels du prototype. Il est également demandé d'évaluer si les acteurs concernés dans l'organisation des élections sont à même de déployer le prototype développé et si les électeurs sont à même de s'adapter à ce nouveau système. À cet effet ont été identifiés les (sous-) processus organisationnels pertinents qui peuvent être influencés par l'introduction du prototype proposé. Chacun des ces sous-processus a été analysé pour pouvoir se forger un jugement sur la faisabilité organisationnelle. L'évaluation des aspects organisationnels du prototype du système a été reprise dans nos rapports du 12 juillet et 20 octobre derniers.

Effectuer les activités de contrôle sur le système pilote de vote

Pour nous exprimer sur le prototype du système de vote, nous avons mené plusieurs activités de contrôle, à savoir des tests fonctionnels, des tests de scénario, des tests de volume, la vérification des spécifications du matériel informatique, l'analyse des fichiers de structure et du code-source, l'évaluation de la documentation, et enfin l'évaluation des points prioritaires. La combinaison de ces tests nous permet de nous exprimer sur l'aptitude du prototype. Les différents types de contrôles et les résultats des tests sont exposés dans le chapitre 4 ÉVALUATION technologique.

Reporting

Le reporting vise l'élaboration du présent rapport lui-même.

3.3 Base de l'évaluation technique du prototype

3.3.1 Logiciel de référence

Nos observations reprises dans le présent rapport sont basées sur les versions ⁵ qui avaient été mises à la disposition de PwC au 30 septembre 2011. Le tableau ci-dessous donne les numéros de version par application :

Application	Numéro de version
Application de préparation	1.2.44_cs.20111130.975
Application de vote	1.3.50
Application du président	1.3.50
Application de totalisation	1.0.0119.20111130.413

3.3.2 Liste des fonctionnalités de base

Pour pouvoir certifier que le prototype est « apte », il doit comporter une série de fonctionnalités de base minimales. Au cours de la réunion du groupe de travail du 24 novembre 2011, une liste exhaustive des fonctionnalités de base a été validée, basée sur le Cahier des charges n° RRN 3/2008. Cette liste est reprise en Annexe D.

3.3.3 Liste de points prioritaires

Pendant le parcours de développement, le pouvoir adjudicateur a été confronté à plusieurs points laissés en suspens ('issues') qui devaient être clarifiés ou résolus. Ces 'issues' ont été consolidés dans une liste ('Master Issue List' ou MIL, cf. Annexe A). Dans la foulée de la certification de la nouvelle version du prototype du système, le groupe de travail et le Groupe d'accompagnement ont fixé des priorités, ce qui a conduit à établir une liste des priorités qui devaient être résolues dans la version du 30 novembre 2011. Pour chacun des points prioritaires, des critères d'acceptation ont été définis entre Smartmatic et les pouvoirs publics. Vous trouverez en Annexe C la liste définitive des points prioritaires telle que définie au cours de la réunion du groupe de travail du 24 novembre 2011.

Le prototype du système doit donc, outre les fonctionnalités de base, offrir également une solution à ces points prioritaires.

⁵ « version » est une combinaison de hardware, de données de tests, de logiciels, d'éléments de configuration et de documentation.

3.3.4 Documents de référence

Comme point de départ de nos activités de contrôle du prototype, nous nous sommes basés sur les documents suivants :

- Le Cahier des charges n° RRN 3/2008 – Cahier des charges spécial pour un nouveau système de vote électronique, du 1^{er} septembre 2008 ;
- L’offre de Smartmatic suite au Cahier des charges spécial RRN3/2008, du 5 octobre 2010 ;
- La note conceptuelle – Concept du nouveau système de vote électronique, du 5 avril 2011 ;
- Les 16 modifications formelles demandées (change requests), du 4 mai 2011, à savoir :
 - Équiper uniquement l’urne électronique d’un lecteur de codes-barres ;
 - Réduire la taille de l’urne électronique ;
 - Du papier plus épais pour l’impression d’un ticket ;
 - Une taille variable des caractères pour le texte lisible sur le ticket ;
 - Dans une circonscription électorale, les tickets doivent toujours avoir la même longueur ;
 - Le scanning des votes via le lecteur de codes-barres par les membres du bureau de vote ;
 - Le non-cryptage des votes émis ;
 - La possibilité d’imprimer en temps réel le scanning des papiers ;
 - Le contrôle de la correspondance du code-barres avec la partie visuelle du ticket ;
 - Un mécanisme de backup pour pouvoir dicter manuellement des bulletins de vote illisibles ;
 - La sécurisation de l’accès par un strip de sécurité ;
 - Le déplacement des connexions USB ;
 - Le recyclage des piles BIOS ;
 - Introduire la piste de vote (smartcard) avec le chip au-dessus ;
 - Un module d’audiovoting est placé en stand-by ;
 - La non-communication des résultats des systèmes de vote ;
- L’étude du Consortium des Universités : « BeVoting – Étude des systèmes de vote électronique, Version 1.02, 4 décembre 2007 » ;
- Les 112 recommandations du Conseil de l’Europe ;
- Les lois et réglementations pertinentes.

S’il y a contradiction entre les documents de référence d’une part et la liste des fonctionnalités de base et la liste des points prioritaires d’autre part, ces dernières ont la priorité.

3.4 Éléments qui sont en dehors du champ d’application du présent rapport

Comme indiqué au point 3.3.3 Liste de points prioritaires, tous les problèmes ou ‘ issues’ connus sont repris dans la Master Issue List (cf. Annexe A). À l’exception de ceux qui ont été désignés comme étant prioritaires (cf. Annexe C), tous les autres ‘issues’ laissés en suspens sont considérés comme n’étant pas nécessaires pour le prototype du système et tombent dès lors en dehors de la portée du présent rapport.

4 Évaluation technologique

4.1 Introduction

Ce chapitre cerne d'abord le cadre technologique au moyen d'un exposé systématique des processus électoraux pertinents. Le cas échéant, les principales modifications par rapport aux versions précédemment évaluées sont mentionnées.

Ensuite, nous précisons notre approche de notre évaluation technologique par un aperçu des activités de contrôle effectuées par nous.

Nous clôturons ce chapitre avec un aperçu de nos observations concernant le prototype.

4.2 Cadre technologique

Avant de procéder à l'évaluation des aspects technologiques du système de vote électronique et du logiciel de vote, les étapes suivantes ont été suivies :

- Identification et définition des (sous-)processus électoraux pertinents ;
- Identification et définition des contrôles qui doivent relever les risques identifiés au sein de chacun des sous-processus.

Cette section contient un aperçu de ces processus et activités.

Le processus de préparation

Un aperçu des processus de préparation et des activités qui y sont liées au sein du prototype est repris dans la figure ci-dessous :

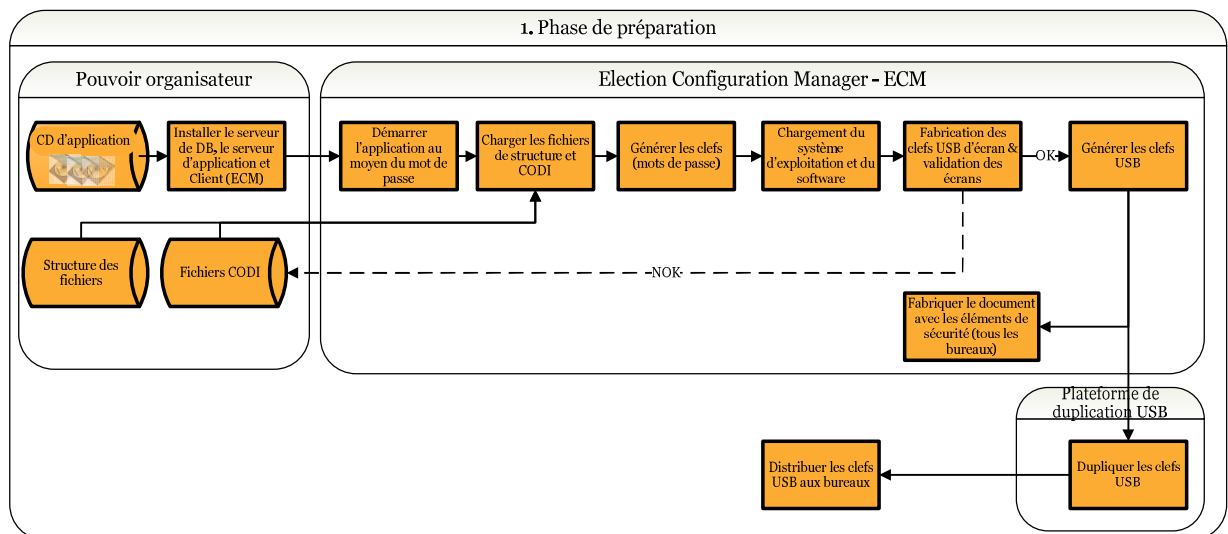


Figure 1: Présentation du processus de préparation

Les étapes qui doivent être franchies au cours du processus de préparation n'ont pas été modifiées par rapport à la solution qui avait été proposée précédemment comme prototype (cf. Le rapport de PwC du 20 octobre 2011). Nous pointons tout de même quelques changements qui sont liés à ce processus :

- l'usage de deux types de duplicateurs, à savoir d'une part un duplicateur de Kanguru Solutions (c'est-à-dire le même type que celui qui a servi pendant l'évaluation précédente en octobre dernier) et d'autre part un duplicateur de US Digital Media ;
- l'usage de nouvelles clefs USB, à savoir le format trapèze ; et
- la manière dont les données sont stockées sur la clef USB 'Master' afin de limiter la redondance des données sur les clefs USB.

À côté des étapes à parcourir nécessairement pour générer une clef USB 'Master', le système de préparation comporte aussi quelques fonctionnalités complémentaires, à savoir :

- la fonction de validation des données chargées via les fichiers de structure. À cet effet sont générés au moyen de règles de mission SQL des rapports sur les informations des données chargées. Ces informations peuvent par exemple être comparées avec ce qu'on avait l'intention de charger pour s'assurer ainsi que le système contient les informations correctes ;
- la fonction de génération des données de test ; et
- la fonction de redécryptage des données cryptées.

Les processus de votes

Par rapport à la solution du prototype précédemment proposé (cf. le rapport de PwC du 20 octobre 2011), le nouveau prototype de système de vote ne comporte pas de modification fondamentale sur le plan de l'émission du vote et du scanning et de l'enregistrement des bulletins de vote. La solution proposée offre deux variantes de scanning :

- Le live-scanning, où l'électeur lui-même doit scanner son bulletin de vote avant de le déposer dans l'urne ; et
- Le post-scanning, où le président scanne tous les bulletins de vote après la fermeture du bureau de vote.

La seule modification au système sur le plan du processus électoral est la possibilité de rouvrir un bureau de vote au moyen d'une carte de secours. Lorsqu'un bureau de vote est ouvert pour la première fois, le président reçoit la possibilité de créer une carte de secours. Il s'agit d'une smartcard, identique à une carte de vote sur laquelle est gravé un mot de passe unique. Si une erreur fatale se produit le jour de l'élection avec les deux clefs USB du bureau de vote, il existe maintenant la possibilité de rouvrir le bureau de vote avec deux nouvelles clefs USB, en combinaison avec la carte de secours. De ce fait il est possible de scanner à nouveau les votes émis lors de la première ouverture du bureau de vote, après la réouverture. Dans les versions précédentes, les votes émis lors d'une première ouverture d'un bureau de vote ne pouvaient absolument plus être scannés si le bureau de vote était rouvert avec des clefs USB non utilisées.

Un aperçu de ces processus de votes et des activités qui y sont liées au sein du prototype pour les deux variantes est repris dans les figures ci-dessous :

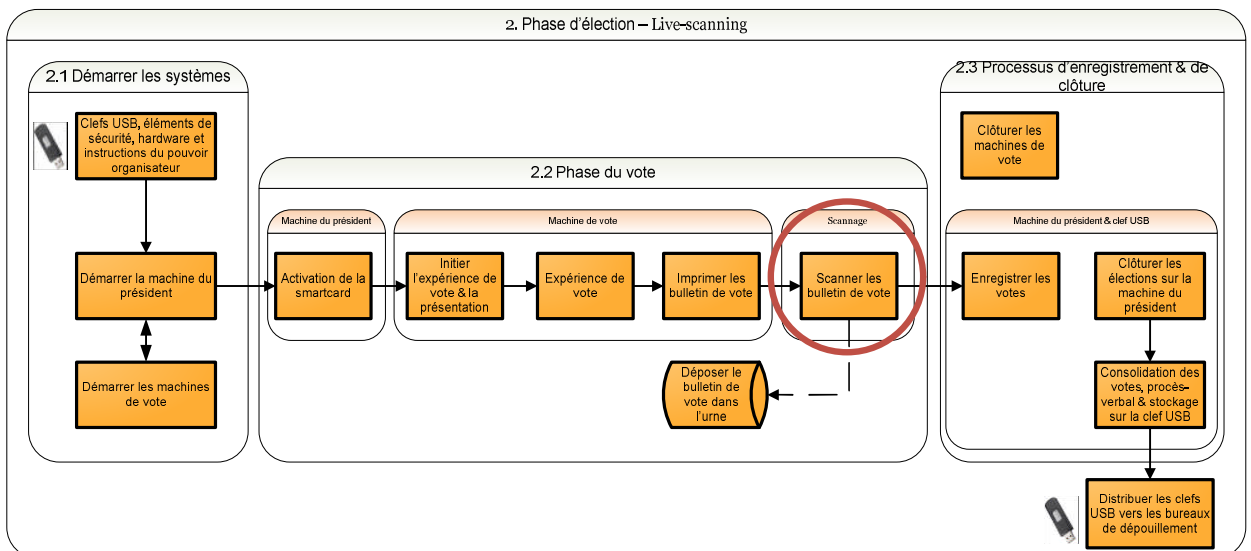


Figure 2: Présentation du processus de votes – Live-scanning

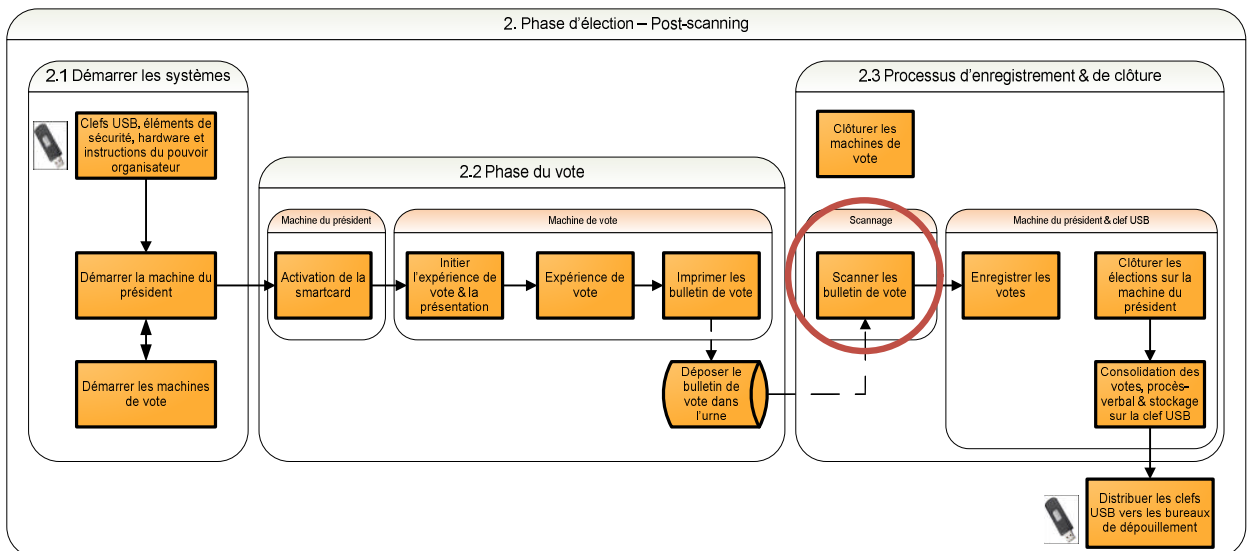


Figure 3: Présentation du processus de votes – Post-scanning

Les processus de totalisation

Un aperçu des processus de totalisation et des activités qui y sont liées au sein du prototype est repris dans la figure ci-dessous :

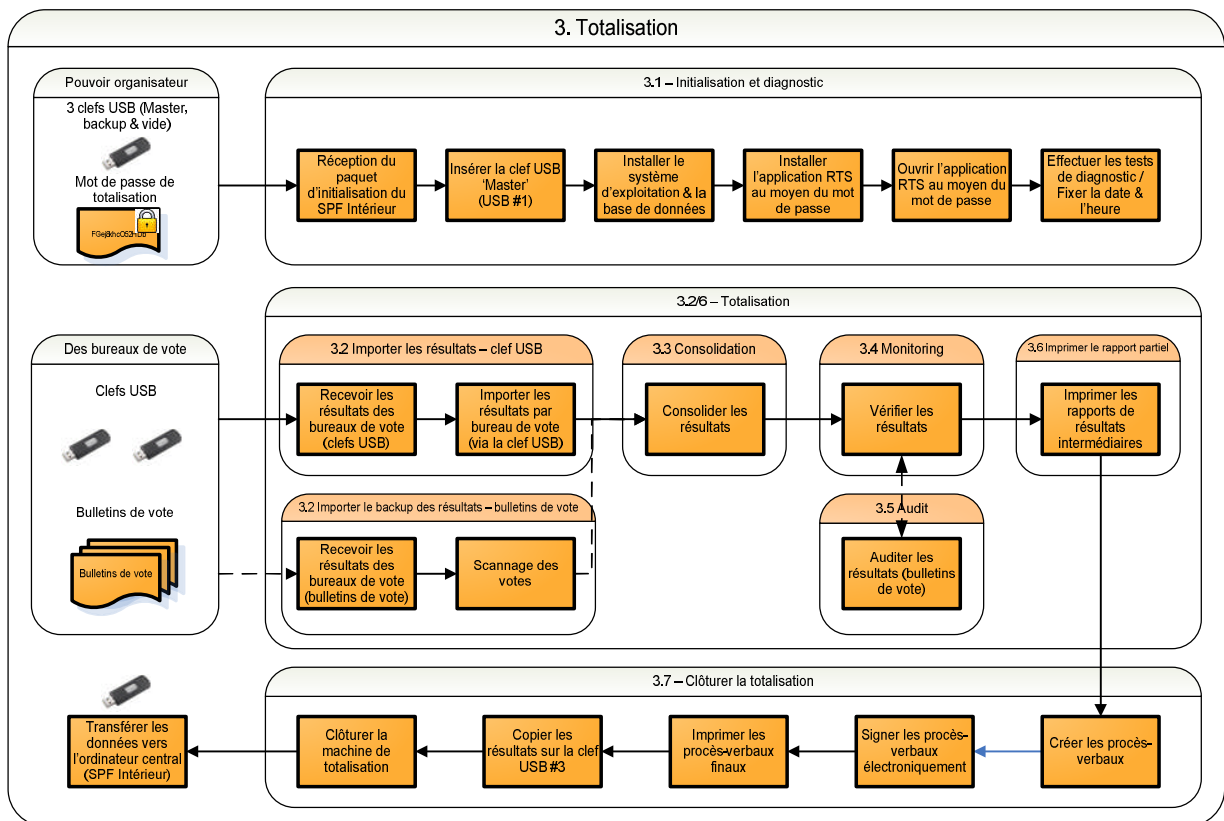


Figure 4: Présentation du processus de totalisation

Par rapport au prototype précédent (cf. le rapport de PwC du 20 octobre 2011), il n'y a pas de modifications fondamentales concernant le processus de totalisation.

Les principales observations des activités de contrôle sur tous ces processus, sur la base de la réalisation de tests détaillés, sont exposées dans la section suivante.

4.3 Approche et observations lors des activités de contrôle du prototype du système de vote

Pour chacun des processus et des activités accessoires, tous les aspects de contrôle attendus ont été identifiés et énumérés en détail dans les cadres de contrôle établis.

À l'aide de ces cadres de contrôle et des plans de tests qui viennent s'y greffer, le prototype proposé et l'application ont été évalués. Lors de ces tests, l'accent est mis sur l'évaluation individuelle des différentes composantes des applications complètes. Les principales observations des activités de contrôle sur tous ces processus, sur la base de l'exécution de tests détaillés, sont décrites dans la section « tests fonctionnels ».

Outre ces tests fonctionnels, d'autres évaluations spécifiques ont été réalisées. Ces activités de contrôle, ainsi que les observations correspondantes, sont décrites dans les sous-sections ci-après.

4.3.1 Tests fonctionnels

Approche

Pour évaluer le fonctionnement (technique) du hardware et des logiciels, un plan de tests détaillé a été dressé pour chacune des parties distinctes du système, à savoir :

- la partie de préparation ;
- la partie du vote, en y distinguant la machine du président et les machines de vote ; et
- la partie de totalisation.

Les plans de tests sont basés sur l'analyse des risques, l'identification des objectifs de contrôle et le système lui-même. Dans l'élaboration des plans de tests, le processus a toujours été suivi et les contrôles attendus ont été identifiés lors des différentes activités sur la base de l'application elle-même, de la documentation et de notre expérience en tant qu'organe d'avis indépendant. Pour chacun des contrôles identifiés, un plan adapté a alors été développé.

Tous les tests des plans de tests qui portent sur le test des fonctionnalités de base et des points prioritaires ont été effectués que le logiciel tel qu'il nous a été fourni les 30 novembre 2011 (cf. 3.3.1 Logiciel de référenc).

Observations

Nos observations résultant des tests fonctionnels ont été reprises de et suivies via la Master Issue List. Pour ces résultats, nous vous renvoyons à la section 4.4 Résultat de l'évaluation technique.

En ce qui concerne la Master Issue List, nous précisons d'une part que nous avons complété cette liste avec nos nouvelles observations et d'autre part que nous avons adapté le statut des points prioritaires sur la MIL et y avons ajouté des commentaires. Étant donné que tous les autres points (non prioritaires) de la MIL sortent du cadre du prototype, nous ne les avons pas explicitement testés à nouveau et nous n'avons pas modifié leur statut dans la MIL, même s'il est possible que certains de ces points aient été entre-temps déjà (en partie) résolus par Smartmatic. La MIL est reprise en Annexe A.

4.3.2 Tests de scénario

Approche

L'objectif des tests suivant certains scénarios préétablis est de vérifier entre autres :

- la mise en œuvre du droit de vote, ou autrement dit chaque type d'électeur (c'est-à-dire, un Belge, un étranger, un Belge vivant à l'étranger) a-t-il accès aux élections auxquelles il peut légalement participer ;
- la mise en œuvre des lois linguistiques, ou autrement dit tous les écrans s'affichent-ils et les rapports s'impriment-ils dans la langue correcte ; et
- la classification et la consolidation des votes émis, ou autrement dit les votes émis sont-ils correctement totalisés et classifiés (par exemple « le nombre de cartes avec des votes pour un ou plusieurs candidats effectifs »).

Les scénarios établis par nous ne recouvrent pas tous les cas « spéciaux ». Dans le temps qui nous était imparti pour l'évaluation, il n'était pas possible de prévoir un scénario spécifique pour chaque particularité. C'est pourquoi, à côté des scénarios choisis, une évaluation a aussi été menée des fichiers de structure. Au moyen de ces fichiers, nombre de comportements du système sont notamment

déterminés. Ainsi dans ces fichiers, sont déterminés par exemple le type d'électeur qui peut participer à chaque type d'élection et le choix de la langue que l'électeur a fait.

Observations

Le tableau ci-dessous donne un aperçu des différents scénarios que nous avons testés, répartis selon la Région. En outre, il est immédiatement précisé dans quels domaines des problèmes se sont présentés. Ceux-ci sont détaillés sous le tableau.

Scénario	Droit de vote	Langue	Totalisation
FLANDRE			
01 – Chambre + Sénat	✓	✓	✓
02 – EU + Région	✓	✓	✓
03 – EU + Région (Heuvelland)	✓	✓	✓
04 – EU + Région (Fourons)	✓	✓	✓
05 – Chambre + Sénat + EU + Région	✓	✓	✓
06 – Chambre + Sénat + EU + Région (Fourons)	✓	✓	✓
07 – Chambre + Sénat + EU + Région (Heuvelland)	✓	✓	✓
08 – Commune + Province + CPAS	✓	✓	✓
09 – Commune + Province + District	✓	✓	✓
10 – Commune + Province	✓	✓	✓
11 – Commune + Province (Bever)	✓	✓	✓
BRUXELLES			
12 – Chambre + Sénat	✓	✓	✓
13 – EU + Région	✓	✓	✗ (1)
14 – Chambre + Sénat+ EU + Région	✓	✓	✓
15 – Commune	✓	✓	✓
WALLONIE			
16 – Chambre + Sénat	✓	✓	✓
17 – EU + Région	✓	✓	✓
18 – EU + Région (Eupen)	✓	✗ (2)	✗ (3)
19 – Chambre + Sénat+ EU + Région (Comines–Warneton)	✓	✓	✓
20 – Chambre + Sénat+ EU + Région (Aubel)	✓	✓	✓

Les cases cochées en vert dans la colonne « Totalisation » signalent le fait que nous avons été à même d'effectuer la totalisation des votes émis dans les différents bureaux de vote et que les résultats tels qu'ils étaient reportés dans les rapports et les PV correspondaient aux votes que nous avons émis. Cependant, les fichiers de résultats de cet exercice de totalisation (le PV final avec l'annexe et les fichiers CODI) ont conduit à plusieurs remarques. D'une manière générale, nous pouvons affirmer que les fichiers d'exportation (les fichiers CODI) ne sont pas entièrement en ligne avec le format de fichier défini pour les fichiers CODI (à savoir le format F).

Nos observations :

- (1) Dans l'annexe au PV pour l'élection du parlement de Bruxelles-Capitale, le nombre de votes blancs n'était pas correctement repris dans la rubrique "Résultats communs pour les groupes linguistiques néerlandais et français". Bien que nous ayons émis pour cette élection sept votes blancs, le nombre de votes blancs était nul selon l'aperçu.

- (2) La mise en œuvre de l'interface de langue allemande n'est pas encore totalement effectuée. En outre les rapports et PV qui sont imprimés pour les communes et cantons germanophones ne sont pas dans la bonne langue.
- (3) Initialement nous n'étions pas à même de clôturer la totalisation d'une commune germanophone. Ce problème a été résolu par l'intervention de SMMT, en modifiant un des fichiers de structure. Nous avons par la suite refait le test avec une clef USB 'Master', créée avec des nouveaux fichiers de structure et n'avons plus constaté de problèmes à ce sujet.

Remarques complémentaires générales :

- Dans l'annexe au PV au niveau de la totalisation, tant de l'élection pour les parlements régionaux que l'élection de la Chambre, le détail manque dans la rubrique « État récapitulatif ». On n'y retrouve que le nombre de carters avec des votes valables, alors que selon le patron officiel (Formulaire AB-25/bis), doivent également être repris le nombre de cartes enregistrées, le nombre de cartes avec des votes blancs et le nombre de cartes avec des votes déclarés nuls.

Pour plus de détails à ce sujet, nous vous renvoyons à la Master Issue List.

4.3.3 Tests de volume

Vu (a) les tests de volume menés précédemment par PwC (cf. Le rapport de PwC du 20 octobre 2011), (b) l'expérience pilote à grande échelle du 27 octobre 2011, où plus de 6.000 citoyens ont testé le système de vote électronique et (c) les tests de volume complémentaires menés par SMMT après l'expérience pilote, où 30.000 votes ont été émis, répartis sur 9 configurations de test (cf. le rapport de Smartmatic « Tests de gros volumes » du 27 novembre 2011, lesquels sont repris en Annexe B), il n'a pas été effectué de tests supplémentaires dans le cadre de nos activités de contrôle pour la certification du prototype.

4.3.4 Analyse des fichiers de structure

Approche

Les fichiers de structure sont utilisés dans le système pour populariser la base de données sous-jacente de l'application. Ces fichiers comportent entre autres la structure de la Belgique, un listing des bureaux de vote et de dépouillement, les clefs de traduction d'une série de notions qui apparaissent sur les écrans, etc., et sont utilisés pour déterminer le niveau auquel la totalisation doit s'opérer (à savoir par commune ou par canton).

Comme ces fichiers influencent le fonctionnement du système, ils ont été soumis à un review. L'accent lors de cette analyse reposait sur la réponse aux questions suivantes :

- La composition des fichiers est-elle simple à comprendre ?
- Les fichiers comportent-ils des informations redondantes ? et
- Les fichiers sont-ils complets ?

Observations

Nous observons que pour plusieurs scénarios, différents sets de fichiers de structure sont nécessaires. Une série de ces fichiers sont les mêmes pour chaque scénario ; d'autres sont spécifiques. Le tableau ci-dessous en donne un aperçu (colonne « Dépendant du scénario ? »). Nous y donnons aussi quelques-unes de nos observations relatives aux fichiers spécifiques reprises dans le tableau.

Fichier	Dépendant du scénario ?	Observations
01 – Category	Non	
02 – Région+NIS	Non	<ul style="list-style-type: none"> • Tous les numéros NIS ne sont pas introduits (car les numéros NIS pour les provinces manquent) • Certains numéros NIS semblent incorrects <ul style="list-style-type: none"> ○ par exemple le canton de Schaerbeek a le même numéro NIS que la commune d'Evere dans le fichier) ○ Par exemple le canton d'Uccle et la commune d'Uccle n'ont pas le même numéro NIS, alors que dans la plupart des cas les cantons et les communes qui portent le même nom ont également le même numéro NIS
03 – Sites	Oui	
04 – Élection	Oui	<ul style="list-style-type: none"> • Ce fichier contient la date des élections (telle que mentionnée sur certains rapports). Celui-ci doit cependant être modifié à chaque élection.
05 – CategoryPath	Non	
06 – District	Non	<ul style="list-style-type: none"> • Les districts de Conseil provinciaux ne correspondent pas à ceux qui sont fixés dans le décret électoral du 8 juillet 2011. Le fichier contient encore l'ancienne répartition des districts de Conseils provinciaux. • Le fichier ne contient pas de données pour les élections communales en Wallonie.
07 – ContestClass	Non	
08 – Contest	Non	<ul style="list-style-type: none"> • Les observations sont les mêmes que pour « 06 – District »
09 – ContestGroup	Oui	<ul style="list-style-type: none"> • Faute d'orthographe : « Deuscht » au lieu de « Deutsch »
10 – Language	Non	
11 – TranslationKey	Oui	
12 – ElectoralAuthority	Oui	<ul style="list-style-type: none"> • Le canton de Merelbeke manque (dans le set de fichiers pour les élections pour la Chambre & le Sénat). De ce fait, aucun nom d'utilisateur et mot de passé n'a été créé pour le bureau de totalisation du canton de Merelbeke.
13 – Profile	Non	
14 – User	Oui	<ul style="list-style-type: none"> • Ce fichier ne comporte que 586 utilisateurs (c'est-à-dire des noms d'utilisateurs pour les centres de totalisation), alors qu'il y a 589 communes en Belgique (dans le set de fichiers pour les élections locales) il manque Gavere, Melle et Oosterzele (dans le set pour les élections locales). De ce fait il est impossible de se « logger » dans le système de totalisation pour ces communes manquantes. • Le canton de Merelbeke manque (dans le set de fichiers pour les élections pour la Chambre & le Sénat). De ce fait il est impossible de se « logger » dans le système de totalisation pour ce canton manquant. D'ailleurs, il n'a pas été créé de nom d'utilisateur et de mot de passe pour ce canton non plus (cf. la remarque sous 12 – ElectoralAuthority).
15 – Keystore	Non	
16 – UP	Non	

Autres observations :

- D'une manière générale, il n'est pas évident de se forger une compréhension complète des fichiers de structure sans documentation technique.
- Il n'est pas tout à fait clair d'appréhender comment les différents fichiers interagissent et quelles clefs doivent être utilisées pour les mettre en liaison.
- Si des modifications doivent être apportées, en lien avec des changements dans la structure de l'État belge, ces modifications doivent être effectuées dans plusieurs fichiers.
- Bien qu'ils soient considérés comme des données statiques, plusieurs fichiers doivent malgré tout être adaptés dans le cadre d'une élection spécifique.

Les observations ci-dessus sont conformes à celles de notre rapport du 20 octobre 2011 et ont déjà été reprises dans la MIL. Par conséquent celles-ci n'ont pas d'impact sur les conclusions concernant le prototype du système.

4.3.5 Analyse du code-source

Approche

Au cours d'évaluations de versions antérieures du prototype du système, le code-source a été évalué sur la transparence et la possibilité de maintenance du code (cf. le rapport de PwC du 20 octobre 2011). Nous avons estimé nécessaire que Smartmatic complète la documentation pour simplifier la transparence et la possibilité de maintenance du code. En outre, nous avons également recommandé que des actions nécessaires soient entreprises pour éviter les éléments suivants : la duplication du code dans le code-source, le code dangereux et les aspects non utilisés.

Le SPF Intérieur a effectué un test complémentaire au moyen du logiciel 'open source' « Sonar »⁶ sur une version du logiciel de Smartmatic du 26 septembre 2011. Sur la base de ce test, une liste de points critiques a été dressée.

Dans le cadre de la certification du prototype, il a été établi lors de la réunion du groupe de travail du 24 novembre qu'il n'y avait pas de points critiques (à savoir ni des points identifiés antérieurement, ni de nouveaux) à rapporter par l'application Sonar dans la version définitive du prototype. Pour le vérifier, une nouvelle analyse a été effectuée sur les versions telles que mises à la disposition de PwC le 30 novembre 2011 par le SPF Intérieur, en présence de PwC le 15 décembre, au moyen du logiciel Sonar.

Observations

L'analyse au moyen de l'outil Sonar a démontré que dans la version actuelle, il ne restait plus que 13 des 130 points critiques initialement identifiés et que quatre nouveaux points critiques sont apparus.

Sept des 13 points critiques initialement identifiés se trouvent dans le paquet "com.smartmatic.security" pour ECM. Bien que ceci soit un paquet commun entre ECM et RTS, le paquet "com.smartmatic.security" ne comporte plus d'erreurs critiques pour le RTS. Cela fait plutôt penser à une négligence qu'à un problème bloquant.

Pour les six autres erreurs, il est évident que Smartmatic a tenté de résoudre ces erreurs, mais Sonar le renseigne toujours comme erreur critique. Celles-ci peuvent néanmoins être résolues de manière simple.

⁶ <http://www.sonarsource.org/>

Trois des quatre nouvelles erreurs critiques concernent deux nouveaux paquets qui ont été ajoutés au code-source. Une quatrième erreur critique se trouve dans un paquet existant. Ces erreurs sont aussi plutôt à mettre sur le compte de la négligence que d'un problème bloquant.

4.3.6 Vérification des spécifications du hardware

Approche

Les caractéristiques des différentes composantes du hardware ont été vérifiées au regard d'une liste de spécifications techniques déclarées par le pouvoir adjudicateur.

Observations

Nous observons à ce propos que les machines de vote qui ont été mises à notre disposition portent encore le logo du fournisseur. Pour le reste les spécifications du hardware sont conformes à la liste des spécifications techniques indiquées par le pouvoir adjudicateur.

4.3.7 Évaluation des points prioritaires laissés en suspens par le passé

Approche

Au cours du parcours de développement, le pouvoir adjudicateur a été confronté à plusieurs points laissés en suspens ('problèmes' ou en anglais 'issues') qui devaient être clarifiés ou résolus. Ces 'problèmes' ont été consolidés dans une liste ('Master Issue List' ou MIL). Dans la foulée de la certification de la nouvelle version du prototype du système, le groupe de travail et le Groupe d'accompagnement ont fixé des priorités, ce qui a conduit à établir une liste des priorités qui devaient être résolues dans le prototype du système à certifier. Pour chacun des points prioritaires, des critères d'acceptation ont été définis entre Smartmatic et les pouvoirs publics. Vous trouverez en Annexe C la liste définitive des points prioritaires telle que définie au cours de la réunion du groupe de travail du 24 novembre 2011.

À côté de l'exécution de notre plan de test et des tests de scénarios, des tests spécifiques ont été menés pour vérifier si les problèmes qui apparaissaient sur la liste prioritaire avaient été résolus. Tous les autres points sur la MIL, à savoir les points non prioritaires ou les problèmes connus, n'ont pas été testés à nouveau explicitement.

Observations

Nos observations résultant de l'évaluation des points prioritaires laissés en suspens ont été reprises et suivies via la Master Issue List.

Plusieurs points prioritaires ne sont pas complètement résolus selon les critères d'acceptation définis, mais nous sommes d'avis que ces points en suspens ne sont pas de nature bloquante. Pour ces résultats nous renvoyons à la section 4.4 Résultat de l'évaluation technique.

Nous précisons que, comme nous ne disposons pas encore de suffisamment d'informations, un point de la liste prioritaire (CusIssP229) reste en suspens. Ce point porte sur la mise en œuvre de l'encryptage asymétrique pour sécuriser les données qui vont du niveau du bureau de vote vers le niveau de totalisation. Notre expert en sécurité continue d'examiner cela et de suivre ce point.

4.3.8 *Évaluation de la documentation*

Approche

L'évaluation de la documentation qui est d'une importance immédiate pour l'utilisateur, comprend deux parties de question :

- la documentation est-elle complète ? (autrement dit : tous les types de documentation requis sont-ils disponibles, la documentation comprend-elle l'ensemble du système) ; et
- quelle est la qualité de la documentation fournie ? (autrement dit : la documentation est-elle dans la langue de lecteur, est-elle concrète et correcte, est-elle claire, etc.).

En outre, la documentation technique et l'analyse doivent être soumises à une évaluation. Celle-ci est principalement focalisée sur sa clarté et son exhaustivité. Le lecteur doit être à même de comprendre le fonctionnement technique du système au moyen de ces documents.

Observations

Observations sur les manuels d'instructions :

- Les manuels ne sont disponibles qu'en anglais. Seules les impressions d'écran reprises dans les documents sont soit en néerlandais, soit en français ;
- D'une manière générale, les manuels sont bien conçus et donnent un aperçu du système étape par étape. Nous observons cependant que ci et là certaines étapes ne sont pas décrites tout à fait comme elles doivent être effectuées dans le système ;
- Il n'est pas toujours évident de savoir quel est exactement le public cible. Bien qu'il s'agisse de modes d'emploi, les documents semblent parfois destinés à un technicien, vu le niveau de détails. D'autre part, il manque à notre avis certains détails qui sont nécessaires pour comprendre le système de manière efficace (par exemple sur le système de totalisation, il faut faire une distinction entre le nom d'utilisateur avec lequel le système doit être installé et le nom d'utilisateur avec lequel le système doit être démarré). De ce fait, il n'est pas toujours aisé de trouver rapidement l'information souhaitée dans le document ; et
- La documentation sur l'ensemble du processus électoral est répartie dans plusieurs documents, qui chacun se focalisent sur une partie du processus ou du système. Un document unique, qui décrit le processus end-to-end, n'est pas disponible.

4.4 *Résultat de l'évaluation technique*

Dans ce chapitre, vous trouverez un aperçu du contenu de nos observations établi sur la base de nos procédures de validation du système de vote fourni à PwC le 30 novembre 2011 (cf. 3.3.1 Logiciel de référence).

Nos observations (ROD) ont été réparties en trois catégories :

- Observations concernant la portée du prototype et qui sont **bloquantes** pour obtenir un avis « apte » ;
- Observations concernant la portée du prototype et qui **ne sont pas bloquantes** pour obtenir un avis « apte » ; et
- Observations qui tombent en dehors de la portée du prototype.

Les sous-sections suivantes comportent un aperçu de nos observations. À ce propos, il y est toujours précisé à quels éléments du logiciel de vote cette observation s'applique (à savoir : le logiciel de préparation, le logiciel pour la machine du président, pour la machine de vote, le logiciel pour la totalisation ou une observation générale). Une description détaillée des observations est reprise en Annexe F.

4.4.1 Observations concernant la portée du prototype et qui sont **bloquantes** pour obtenir un avis « apte »

Il n'y a pas d'observations bloquantes constatées concernant une des fonctionnalités de base (cf. section 3.3.2 et Annexe D) et/ou un élément de la liste des points prioritaires (cf. section 3.3.3 et Annexe C)

4.4.2 Observations concernant la portée du prototype et qui **ne sont pas bloquantes** pour obtenir un avis « apte »

Le tableau ci-dessous donne un aperçu des observations non bloquantes concernant le prototype.

Nous observons que les ROD relatives au système de totalisation (cf. colonne « Module ») n'ont pas d'influence sur l'organisation des élections locales en Flandre (octobre 2012), vu que pour la Flandre, une interface entre la machine du président et le système CODI sera développée et que le système de totalisation actuel proposé par Smartmatic ne sera pas utilisé.

N° ROD	Observation	Module	Référ. MIL
ROD-001	La redondance de données sur la clef USB 'Master' concernant les fichiers election.xml peut encore être diminuée, afin de gagner du temps pendant le processus de préparation.	Préparation	CusIssPr174
ROD-002	Il n'y a pas de fichiers PDF des écrans de dialogue créés pendant la création des écrans sur l'application ECM.	Préparation	CussIssPr167
ROD-003	Il n'y a pas de "log" convivial présent des modifications apportées via la fonctionnalité "change candidate names".	Préparation	CusIssPr193

N° ROD	Observation	Module	Référ. MIL
ROD-004	Les tests de diagnostic ne sont pas tout à fait conformes aux critères d'acceptation.	PC du président PC de vote Totalisation	CusIssGen004, CusIssP280, CusIss076, CusIss134, CusIss233, CusIssT016
ROD-005	L'application RTS n'est pas toujours stable dans un usage normal.	Totalisation	CusIssT226, CusIssT239
ROD-006	Lorsqu'on retire la clef USB master, cela ne s'indique pas sur les PC 'esclaves' du même réseau.	Totalisation	CusIssT239
ROD-007	Il n'y a pas de confirmation obligatoire de la date et de l'heure après s'être connecté dans l'application RTS.	Totalisation	CusIssT259
ROD-008	Les procès-verbaux et les fichiers de résultats exportés au niveau de la totalisation contiennent encore des erreurs.	Totalisation	CusIssT195
ROD-009	Le hardware a présente parfois un comportement instable pendant l'exécution des plans de test.	Général	CusIssT226
ROD-010	L'usage de la carte E-ID pour signer les procès-verbaux au niveau de la totalisation n'est pas conforme à la politique des cartes E-ID	Totalisation	CusIssT173, CusIssT262

4.4.3 Observations qui tombent en dehors de la portée du prototype

Durant les évaluations actuelles et antérieures, une série de problèmes ont été constatés qui tombent en dehors de la portée du prototype. Pour un aperçu de ces problèmes, nous renvoyons à la MIL (cf. Annexe A). Cette catégorie de problèmes ne fait pas l'objet d'un tableau spécifique des observations dans le présent rapport.

5 *Aspects organisationnels*

Dans nos précédents rapports (cf. le rapport de PwC du 12 juillet 2011 et le rapport de PwC du 20 octobre 2011), a été examiné l'impact organisationnel du nouveau système de vote automatisé proposé. Y ont été passés en revue les processus organisationnels et les acteurs concernés par le processus électoral et il y était donné une indication du temps (techniquement) nécessairement pour réaliser les différentes étapes du nouveau système de vote.

Ce chapitre comporte d'une part une mise à jour du temps (techniquement) nécessaire pour la réalisation du processus de préparation et l'ouverture des bureaux de vote et reprend d'autre part le calcul du nombre de bureaux de vote nécessaires au minimum pour le traitement de 2.000 électeurs dans le laps de temps d'ouverture des bureaux de vote (de 8 h. à 15 h.).

5.1 Temps techniques liés au prototype du système

Le tableau ci-dessous reflète le temps (techniquement) nécessaire pour réaliser le processus de préparation et l'ouverture des bureaux de vote avec le prototype actuel du système, qui a été fourni le 30 novembre, par comparaison avec le prototype antérieur qui avait été fourni le 30 septembre.

Il faut préciser à ce propos que dans le nouveau système, les clefs USB doivent d'abord être formatées, c'est-à-dire dupliquées avec une clef USB 'blanche' (fournie par Smartmatic), avant de pouvoir commencer la duplication de la clef USB 'Master' générée. Ce processus a été évalué pour les deux duplicateurs qui ont été mis à notre disposition : l'Accutower et le Kanguru. L'Accutower comporte 35 ports USB, ce qui signifie qu'il est possible de dupliquer 34 clefs USB. Dans le cas de duplication de la clef 'blanche', ce processus nécessite 40 secondes. Le Kanguru comporte 43 ports USB, soit la duplication de 42 clefs USB. Ici, le processus dure 2 minutes.

Les temps repris dans ce tableau sont basés sur un scénario d'élections simultanées pour les parlements fédéral, régional et européen (c'est-à-dire le « scénario 2009 + 2010 »).

Pour une description textuelle détaillée des différentes étapes, nous renvoyons à nos précédents rapports.

	Mesure précédente du temps sur le système de vote - version du 30 septembre (cf. le rapport de PwC du 20 octobre 2011)	Mesure actuelle du temps
1. Conception et approbation des impressions d'écran		
1.A Chargement des données & des programmes et création des mots de passe		
Chargement des fichiers de structure (fichiers 'txt')	0 h. 06 min.	0 h. 06 min.
Chargement des fichiers CODI	0 h. 07 min.	0 h. 07 min.
Chargement du système d'exploitation et du logiciel	0 h. 02 min.	0 h. 02 min.
Création des mots de passé	3 h. 50 min.	0 h. 25 min.
Durée totale des étapes ci-dessus	4 h. 05 min.	0 h. 40 min.
1.B Initialisation de la clef USB de génération d'écran		
Initialisation d'une seule clef USB pour toute la Belgique et génération d'écrans sur une seule machine de vote	0 h. 55 min.	0 h. 11 min.
Initialisation de plusieurs clefs USB, chacune pour un territoire plus restreint (par exemple une province) et générer en parallèle des écrans sur plusieurs machines de vote	0 h. 55 min.	0 h. 07 min.
1.C Générer les impressions d'écran au moyen de la clef USB de génération d'écran		
Générer les écrans via une seule clef USB pour toute la Belgique	105 heures	2 h. 30 min.
Générer les écrans via une seule clef USB pour une province (ici la province d'Anvers)	6 h. 05 min.	0 h. 15 min.
Traitement des écrans par le système de préparation pour toute la Belgique	Pas de mesure	0 h. 10 min.
Traitement des écrans par le système de préparation pour une province	0 h. 15 min.	0 h. 06 min.

	Mesure précédente du temps sur le système de vote - version du 30 septembre (cf. le rapport de PwC du 20 octobre 2011)	Mesure actuelle du temps
2. Initialisation et duplication de la clef USB 'Master'		
2.À Chargement des données & des programmes et création des mots de passe (conditionnel)		
Idem que sous 1.À, mais uniquement à exécuter si des modifications doivent être apportées aux impressions d'écran	4 h. 05 min.	0 h. 40 min.
2.B Initialisation de la clef USB 'Master'		
Générer la clef USB 'Master'	5 h. 25 min.	5 h. 03 min.
2.C Duplication de la clef USB 'Master'		
Duplication de 42 clefs USB sur le duplicateur de la firme Kanguru Solutions (hors insérer et retirer les clefs USB)	20 à 40 min. (plusieurs mesures)	7 min. (20 clefs)
Duplication de 34 clefs USB sur le duplicateur de la firme US Digital Media (AccuTower) (hors insérer et retirer les clefs USB)	Duplicateur non disponible	4 min. (20 clefs)
2.D Duplication de la clef USB 'blanche' = formatage		
Duplication de la clef USB 'blanche' sur le duplicateur de la firme Kanguru Solutions (en dehors d'insérer et retirer les clefs USB)	Pas de mesure	2 min. (20 clefs)
Duplication de la clef USB 'blanche' sur le duplicateur de la firme US Digital Media (AccuTower) (en dehors d'insérer et retirer les clefs USB)	Duplicateur non disponible	40 sec. (20 clefs)

	Mesure précédente du temps sur le système de vote - version du 30 septembre (cf. le rapport de PwC du 20 octobre 2011)	Mesure actuelle du temps
3. Démarrage de la machine du président et des machines de vote		
Temps total de démarrage des machines = (a) + 5*(b)	16 min. 15 sec.	19 min. 30 sec.
Démarrage de la machine du président (a)	4 min. 35 sec.	5 min. 20 sec.
Démarrage des machines de vote (b)	2 min. 20 sec.	2 min. 50 sec.
Composition du bureau de vote (uniquement le président et le secrétaire)	2 min. 00 sec.	2 min. 00 sec.
Réalisation du test d'acceptation par le président (pour 5 machines de vote)	6 min. 40 sec.	6 min. 00 sec.
Ouverture des élections sur la machine du président	1 min. 00 sec.	1 min. 00 sec.
Temps total nécessaire pour le démarrage et l'ouverture d'un bureau de vote	25 min. 55 sec.	28 min. 30 sec.
4. Activation de la carte de vote		
Activation de la carte de vote	3 – 4 sec.	3 – 4 sec.
Procédure d'enregistrement d'une carte de procuration /d'assistance (sans objections)	3 min.	3 min.
Enregistrement d'une objection	2 min.	2 min.

5.2 Nombre de machines de vote nécessaires par bureau de vote

Comme il est prescrit par l'article 142 du Code électoral, les électeurs sont autorisés dans le bureau de vote le jour de l'élection de 8 heures à 13 heures. En outre, la loi organisant le vote automatisé prescrit à l'article 14, paragraphe 3, que le Roi peut prolonger les heures d'ouverture des bureaux de vote. Si tel est le cas, les instructions (disponibles sur le site internet du SPF Intérieur) sont modifiées pour l'électeur. Ces instructions, telles qu'elles sont établies par exemple pour les élections de 2010,⁷ stipulent que les bureaux de vote avec le vote automatisé sont ouverts jusqu'à 15 heures.

Cela signifie que chaque machine de vote est disponible pendant 7 heures pour exécuter l'élection. En fonction du nombre de machines de vote disponibles, cela représente une disponibilité totale de 7 heures multipliées par le nombre de machines disponibles (par exemple 35 heures si 5 machines sont disponibles).

Sur la base des décrets / lois actuels⁸ suivants, nous posons que :

- En Belgique (à l'exception de l'arrondissement de Bruxelles-Capitale), le nombre maximum d'électeurs par isoloir (indirectement donc par machine de vote) est fixé à 180. Dans l'arrondissement de Bruxelles-Capitale, le nombre maximum d'électeurs par isoloir est fixé à 160.
- Le nombre maximum d'électeurs par bureau est fixé à 800 si on vote avec un bulletin de vote. Le pouvoir organisateur peut, si le vote se déroule autrement qu'au moyen d'un bulletin de vote, augmenter le nombre d'électeurs par bureau de vote sans cependant que ce nombre excède 2.000.

Implicitement, la législation existante comporte qu'en Belgique (à l'exception de l'arrondissement de Bruxelles-Capitale), le nombre maximum d'électeurs par isoloir (indirectement donc par machine de vote) est fixé à 900 (dans un bureau de vote avec 5 machines de votes). Le Cahier des charges spécial comporte aussi la question de savoir si un bureau de vote est aussi à même de traiter 2.000 électeurs dans le laps de temps de l'ouverture des bureaux de vote.

Au moyen des chiffres ci-dessus ont été dressés les aperçus suivants. Ce schéma montre le nombre moyen de secondes que l'électeur a à sa disposition pour émettre son vote.

⁷

http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections2011/fr/officiel/instructions/13_ELECT_Anticipaes_VoteAuto_20090818_F.pdf

⁸ Décret électoral provincial actuel – Article 2 ; Code électoral – Article 90 ; Décret électoral communal – Article 8

Situation en Belgique, à l'exception de l'arrondissement de Bruxelles-Capitale :

Nombre de machines de vote		4	5	6	7	8	9	10	11	12
Nombre d'électeurs	800	126	158	189	221	252	284	315	347	378
	900	112	140	168	196	224	252	280	308	336
	1000	101	126	151	176	202	227	252	277	302
	1100	92	115	137	160	183	206	229	252	275
	1200	84	105	126	147	168	189	210	231	252
	1300	78	97	116	136	155	174	194	213	233
	1400	72	90	108	126	144	162	180	198	216
	1500	67	84	101	118	134	151	168	185	202
	1600	63	79	95	110	126	142	158	173	189
	1700	59	74	89	104	119	133	148	163	178
	1800	56	70	84	98	112	126	140	154	168
	1900	53	66	80	93	106	119	133	146	159
2000	50	63	76	88	101	113	126	139	151	

Situation dans l'arrondissement de Bruxelles-Capitale :

Nombre de machines de vote		4	5	6	7	8	9	10	11	12	13
Nombre d'électeurs	800	126	158	189	221	252	284	315	347	378	410
	900	112	140	168	196	224	252	280	308	336	364
	1000	101	126	151	176	202	227	252	277	302	328
	1100	92	115	137	160	183	206	229	252	275	298
	1200	84	105	126	147	168	189	210	231	252	273
	1300	78	97	116	136	155	174	194	213	233	252
	1400	72	90	108	126	144	162	180	198	216	234
	1500	67	84	101	118	134	151	168	185	202	218
	1600	63	79	95	110	126	142	158	173	189	205
	1700	59	74	89	104	119	133	148	163	178	193
	1800	56	70	84	98	112	126	140	154	168	182
	1900	53	66	80	93	106	119	133	146	159	172
2000	50	63	76	88	101	113	126	139	151	164	

En prenant ces résultats en considération, PwC a effectué 10 fois le même vote pour une combinaison d'élections (élections fédérales + élections régionales + élections européennes). La durée moyenne de ces 10 votes a été fixée à 60 secondes.⁹ Il est important de noter ici que cette indication de temps comprend l'expérience de vote complète (à savoir la durée pendant laquelle l'électeur se trouve dans l'isoloir). Si nous ne considérons que l'opération de vote (à savoir le choix des candidats pour l'élection concernée), il a été estimé que cela prend en moyenne 35 à 40 secondes.

Pour l'interprétation des tableaux ci-dessus, on a utilisé les codes de couleur suivants :

⁹ Cette indication de temps n'est qu'une estimation. Il est souhaitable que le pouvoir organisateur évalue cette indication de manière critique, sûrement si plusieurs élections sont organisées simultanément.

- Le vert indique les combinaisons possibles qui répondent à l'exigence légale minimale du nombre de machines de vote (par exemple, s'il y a 800 électeurs par bureau de vote, il faut au minimum 5 machines de vote) ;
- L'orange indique que les combinaisons possibles ne répondent pas à l'exigence légale minimale du nombre de machines de vote. Cependant, ces combinaisons offrent un nombre de secondes disponibles plus élevé pour émettre un vote que les 60 secondes calculées. **Error! Bookmark not defined.** En d'autres mots, ces combinaisons offrent une opportunité à tous les électeurs d'émettre leur vote avec un plus petit nombre de machines de vote qu'exigé par la législation (moyennant une modification de la loi) ;
- Le rouge indique les combinaisons qui ne répondent pas aux exigences légales (quant au nombre maximum d'électeurs par isoloir), et n'ont pas un nombre moyen suffisamment élevé de secondes disponibles pour permettre à tous les électeurs d'émettre leur vote.

Vu qu'une autre machine de vote sera aussi disponible, pourvue d'un scanner de codes-barres, pour permettre à l'électeur de revoir son vote, il faut aussi poser que, partant des hypothèses les moins favorables, il est possible qu'il y ait une machine de vote en moins disponible pour l'expression des votes. Il est dès lors opportun de prendre cette observation en compte lors de la fixation du nombre de machines de vote nécessaires par bureau de vote.

Il est important que le pouvoir organisateur prenne acte de ces indications de temps lors de l'organisation des élections. Une vigilance accrue est certainement souhaitable dans l'hypothèse où plusieurs élections sont organisées simultanément.

Annexes

Aperçu :

Annexe A – Aperçu MIL

Annexe B – Rapport de Smartmatic « Tests de gros volumes » du 27 novembre 2011

Annexe C – Liste des points prioritaires

Annexe D – Liste des fonctionnalités de base

Annexe E – Rapport d'évaluation du code-source avec l'outil Sonar

Annexe F – Rapports d'observations détaillés (ROD)

Annexe A – Aperçu MIL

Nous renvoyons à ce propos au spreadsheet de l'aperçu « Appendix A_Bevoting MIL Prototype_20111220_final.xlsx », joint à la version électronique de ce rapport.

Annexe B – Rapport de Smartmatic « Tests de gros volumes » du 27 novembre 2011

Nous renvoyons à ce propos au document « Appendix B_HVT_VotePrintScan30K_SMTT_9-25Nov_v1_0.pdf », joint à la version électronique de ce rapport.

Annexe C – Liste des points prioritaires

MIL reference	Issue description
CusIssGen002	For the moment, the system cannot yet be used for the organization of all possible legal combinations of elections in Belgium
CusIssGen004	The diagnosis verification of all the different components in the entire process cannot be performed with a USB key that was especially provided for that reason: * Diagnosis before organizing the elections - open * Diagnosis at the level of the individual
CusIssGen021	the source code is too complex. It is necessary to rewrite it "from scratch"
CusIssPro12	Creating the master USB takes a long time (better if we work with servers?)
CusIssPro86	Validation on the data that is imported should be improved. Importing wrong, missing or incomplete data is only detected when generating the usb key.
CusIssPr149	We noted that the pdf files created by the screen generator functionality does contain the name of the first polling station. The name of the "kieskring" must be printed instead Update 19/10 : in addition the PDF with the screens contain page numbers but not per circonscription
CusIssPr167	The pdf file generated of the Screen Shot Image doesn't have all images of the voting experience
CusIssPr174	All lists of candidates should be kept only once on the USB, in stead of one copie per polling place. This can have an influence on the capacity required on the USB and the time required to generate the USB. In addition, validation steps for imported data should be build in, before the start of the time consuming processes.
CusIssPr178	We noted no changes in the implementation of the screen generator. It is still a very time consuming process. All screens are generated for one polling place in each commune. We generated the screens for 2009-2010 elections and we noted that the screens are not generated per circumscription (checked in the USB stick coming from the VM). Moreover, we noted that the screen generation on the VM took approximately 102 hours for 2009-2010 elections (full of Belgium). Furthermore, during the generation of the screens we noticed that some screens are generated more than once. We were not able to process the generated screens on the PREP machine.
CusIssPr180	The 'enforced' workflow is not accurately implemented. We noted some issues with the navigation: - Going to a previous from the password generation results in the removal of all passwords and keys. (needed for time saving while generating the screens on VM's as this step is performed before the generation of the passwords). - Navigation between the first (upload static and CODI) and second step (upload of images) requires to perform the post treatment of the CODI files. This should be part of the upload of CODI.
CusIssPr182	There is no automatic check on the hash code (CODI + Images). Hence manual procedures should be in place to cover the risks. For municipalities elections there are a lot (!) of CODI files to be loaded (> 300 files for Flanders only).
CusIssPr193	It is not possible to change an individual static data file or CODI file during the preparation process. If one file needs to be replaced, all files need to be uploaded again (txt or CODI respectively) after removing all of them first.
CusIssP073	The diagnosis verification of the different components in the voting system (President Machine) are inadequate or not clear enough
CusIssP087	In case the PM self-diagnose check identifies a damaged/failing HW component, this does not halt the installation process. Furthermore, the error information message disappears fast & President can miss this message.

MIL reference	Issue description
CusIssP195	USB sticks connectivity to president machine - should also work with 1 USB connected except for the start of the scanning of the ballots for which always 2 USB sticks are required
CusIssP229	OBR 3.6_1 PM - Additional security mechanisms have to be implemented. To date, the system has still adequate security mechanisms yet to be implemented. For example: The result file in the USB from the polling place is encrypted with a symmetric key and electronically signed. This is not a sufficient level of security to prevent changes in the content of the USB, because both the symmetric key and the private key used for encryption and signing correspondingly are accessible in the USB by the returning officer.
CusIssP280	Diagnoses in maintenance menu not working properly - Printer diagnose does not notice that the printer is out of paper. - A crash occurred during "all diagnoses" when the printer is disconnected. - USB key can be removed and still a successful diagnose of USB. - No suggested solutions
CusIss076	During the diagnosis, the process doesn't continue as long as no paper is in, and the message that is displayed is not appropriate
CusIss134	The diagnosis verification of the different components in the voting system (Voting Machine) are inadequate or not clear enough
CusIss142	A fail in the diagnostic check does not stop the installation, hence the President could miss the message.
CusIss233	Diagnose only mode - Functionalities are not working properly. E.g. - Barcode reader always fails if printer is out of paper - Barcode printed can not be read by barcode reader. - Machine does not notice near end of paper, end of paper is indicated as a fail (without further explanation) - Usability: at start-up the system does not indicate to touch the points on screen (red dot in blue circle). - No suggested solutions.
CusIss235	Diagnose only mode - One USB per language. Would be better to give the user the choice. Also applicable to PM!
CusIss255	Diagnose functionalities are not working properly. E.g. - Barcode reader always fails if printer is out of paper and the system crashes. - Barcode printed can not be read by barcode reader. - Machine does not notice near end of paper, end of paper is indicated as a fail (without further explanation) - Layout of the printed report is NOK (issues with line returns) - No suggested solutions.
CusIss261	We noted two cases where the name of the candidate did not fit in the box on the screen of the voting machine.
CusIssTo16	The diagnosis verification of the different components in the totalisation system (totalisation machine) is inadequate or not clear enough
CusIssTo36	Issues encountered for diagnostic checks of barcode reader, USB ports and SmartCard reader. If a check is successful, but the user then creates a failed check, the status remains "successful".

MIL reference	Issue description
CusIssT173	<p>OBR 2.1 PM - When closing the polling station, the president machine creates a result file that contains the result of the votes for that specific polling station. This file, which will be read by the totalisation system afterwards, doesn't have to be signed with the eID of the president of the polling station, contrary to the description in the BAFO and the requirements of the concept note. The information of the eID is read and registered, but the information can be overwritten afterwards. In addition, the use of the pincode of the eID is not required to digitally sign the file.</p> <p>When finalising the totalisation, the totalisation machine creates a result file that contains the result and that serves as an input file for the central computer system. This file doesn't have to be signed with the eID of the president of the totalisation office, contrary to the description in the BAFO. The information of the eID are read and registered, but can be overwritten afterwards. In addition, the use of the pincode of the eID is not required to digitally sign the file.</p>
CusIssT195	<p>OBR 3.24 TOT - CODI file exported with results is incomplete and not in line with format F.</p> <ul style="list-style-type: none"> -Prefix "DC" cannot be used for results, but for final lists of candidates. -For the election of the members of the Flemis Parliament in Brussels, type of election is not correct (VL instead of BV) in line "G" and the type of office the list is not correctly finalized (C instead of R) in line "S". -Numbers of valid, registered blank/invalid votes and the total control field missing from line "S". -Aggregated votes and the sum-rate control field missing in line "L". -Special characters used in text fields, even for candidates and parties (not in accordance with requirements 437/DOS page table code). -Candidates are not properly sorted (e.g. candidate 10, then 11, then 1). -Lists are not sorted by vote, but by the "order of filling". -"T" line is missing. -Misscategorization of votes. Please see OBR 1.5.
CusIssT196	<p>OBR 3.25 TOT - If 2 USBs from the same polling place, with different results exist, the procedure followed by the TOT system is to keep the results of the first one scanned only. The system should ask the system which set to keep.</p>
CusIssT199	<p>OBR 3.27_1 TOT - Not all PVs and reports are exported (e.g. The "View a List" report in Dutch in the election of the Brussels Parliament. The "Blanks and List" report either.</p>
CusIssT226	<p>RTS application has stability issues. E.g.</p> <ul style="list-style-type: none"> - When entering the usb stick in order to totalise the results, the TOT master pc crashed and no error message was displayed. - Diagnose functionality blocked the system - Difficulties entering the back-up mode - After having totalized 5 polling places, the pc crashed - When closing the totalisation, the pc crashed
CusIssT239	<p>After the error message, shown when trying to close the totalisation without the backup USB stick inserted, is displayed, the system is blocked and has to be restarted, although no error message was given. Furthermore:</p> <ul style="list-style-type: none"> - in some cases, we were unable to close the totalisation normally afterwards; - in some cases, the system did not recognize the USB stick anymore after restarting the application. <p>Therefore we had to reinstall the application on another TOT pc which succeeded in the end, although all results were gone (no recovery option was given; it started up as master TOT pc immediately).</p>
CusIssT243	<p>It is not possible to perform a successful diagnose test of the smartcard reader. The "Diagnose" button of the smartcard reader diagnose is not usable and the message that the diagnose test failed is already shown in the "Progress" text field without performing the diagnose test. Furthermore, a red cross is displayed in the diagnose overview (when clicking "Terug" after the test).</p>

MIL reference	Issue description
CusIssT258	<p>A network can be configured by connecting all the TOT pc's via network cables to a hub (and checking if the lights are lit) and installing these one by one. The first installed TOT pc is always configured as the master TOT pc (an 'eausrXXX.xml'-file is created in the folder '/data/conf' on the master USB stick).</p> <p>After installation of the master TOT pc (not logged in yet), the other TOT pc's need to be booted with the same master USB stick (one by one). After this, the user has the option to select the icon of the master, slave or recovery mode. When selecting the slave icon, the pc is configured as slave TOT pc. However, when selecting the Master icon, it is possible to initialise a second Master in the network.</p>
CusIssT259	<p>We noted that when the back up USB stick is removed from the master TOT pc before a back up moment and only after this back up moment inserted again, the system does not reconcile nor notifies the user (by means of a message) in case of an inconsistency between hard drive and back up USB stick. This means that back ups on the USB stick can be avoided. Since the last 3 back ups can be used for recovery purposes, this means that data could be potentially lost.</p>
CusIssT262	<p>As a consequence to the known-issue, we noted that, although a pop up with the question to close by means of eID or not is given, it is not possible to use a Belgian e-ID card to close the totalisation process and the message asking the user to insert an eID card (even though it is inserted), is displayed. When clicking 'OK' multiple times (because this message keeps on showing up), the system proceeds to the pop up to enter the data of the members of the totalisation bureau without closing and/or signing by means of a Belgian eID card.</p>

Annexe D – Liste des fonctionnalités de base

Les fonctionnalités de base qui sont nécessaires pour le prototype sont celles qui sont indiquées **en gras et italiques** dans l'extrait repris ci-dessous du Cahier des charges portant la référence RRN 3/2008. Les éléments en grisé et barrés ne sont pas considérés comme étant des fonctionnalités de base et ne sont donc pas requis pour le prototype du système. Les éléments qui sont repris en **gras, italiques et soulignés** ont été ajoutés dans l'extrait et ne figuraient pas dans l'offre initiale.

Extrait du Cahier des charges (section « D.A.1. Les prestations du lot 1 – Poste 1 : » pages 41-46) :

« Le poste 1 vise à la fourniture d'un nouveau système de vote électronique offrant à la fois la possibilité d'un contrôle papier et la possibilité d'enregistrement électronique du vote. Ce qui inclut :

- **Développement d'un prototype de système de vote électronique dont vous trouverez une description non exhaustive jointe ci-après à titre informatif :**

Le prototype se compose de tous les appareils qui sont nécessaires à l'exécution du processus électoral.

~~Le fournisseur est responsable de la fourniture du matériel nécessaire.~~

~~Le prototype doit prévoir la possibilité pour les aveugles et malvoyants de pouvoir voter si possible en toute autonomie.~~

~~Le prototype doit être contrôlé et agréé par un organisme agréé. Les tests de l'organisme de contrôle doivent être suffisamment larges et approfondis. L'organisme de contrôle présentera son programme de test à l'autorité.~~

Il doit également être développé un software qui peut démontrer que toutes les fonctionnalités fonctionnent correctement. Celui-ci doit pouvoir également être utilisé lors de l'exécution du contrôle ultérieur des appareils.

- ~~Exécution d'une étude de faisabilité~~

~~L'étude de faisabilité comprend une étude de la viabilité à grande échelle du prototype et d'une analyse de risque.~~

~~Tâches~~

~~L'étude de faisabilité doit analyser l'étude du Consortium d'universités ainsi que le prototype.~~

~~Tant l'étude que le prototype doivent être analysés quant à la viabilité technique de tout le processus électoral.~~

~~Les points suivants devront en particulier être examinés:~~

- ~~— Le système est-il conforme à la législation en matière d'emploi des langues et aux législations électorales ?~~
- ~~— Le système est-il conforme aux dispositions du Conseil de l'Europe (<https://wed.eoe.int/ViewDoc.jsp?id=778189>) ? Dans la négative, quelles sont les actions à entreprendre pour y remédier ?~~
- ~~— Le système satisfait-il au principe de *free and fair elections* : droit de vote général, secret, égal, libre et non discriminatoire ?~~
- ~~— Quel est le prix coûtant du système ?~~
- ~~— Y a-t-il suffisamment d'éléments de sécurité, de contrôles et de systèmes de back-up prévus ?~~
- ~~— Quels sont les aspects organisationnels et le système est-il exécutable pratiquement ?~~
- ~~— Les élections peuvent-elles être organisées en 40 jours ?~~
- ~~— Combien de citoyens seront appelés pour siéger dans les différents bureaux ?~~

Nouveau système de vote électronique : Avis concernant l'aptitude du prototype

- Le système conviendrait-il à l'organisation simultanée de plusieurs élections ?
- Le bureau de vote est-il à même de traiter 2000 électeurs sur la durée d'ouverture des bureaux de vote (8 h. - 15 h.) ? De combien de temps un électeur moyen a-t-il besoin pour exprimer son vote ?
- Combien de temps requiert une production complémentaire de matériel électoral ?
- Quels services peuvent être sous-traités à un prestataire de services ?
- Le système est-il accessible aux personnes moins valides ?
- Le système répond-il aux exigences techniques ?
- Le système répond-il aux exigences fonctionnelles ?
- Le système répond-il aux exigences en matière de sécurité et de disponibilité ?
- Le système répond-il aux exigences en matière de gestion et de maintenance ?
- Le système répond-il aux exigences en vue de son utilisation par les instances chargées de l'organisation des élections ?
- Le système répond-il aux exigences en vue de son utilisation par l'électeur ?
- Quel est l'impact sur les facteurs liés à l'environnement ?

Il doit également être procédé à une analyse de risque approfondie sous la forme d'un tableau. Celui-ci comprend entre autres une étude sur les rayonnements électromagnétiques et leurs conséquences.

- **Prototype de vote compatible avec les procédures de vote non exhaustives décrites ci-après et jointes à titre informatif :**

Toutes les procédures et tâches dans les différents bureaux doivent pouvoir être accomplies simplement et rapidement de sorte qu'un minimum de citoyens doivent y être convoqués.

1. Procédure de génération

Au cours de la procédure de génération, il peut être fait usage d'un appareil de génération pour créer un support qui sera utilisé pour pouvoir initialiser de manière sécurisée et différenciée tous les bureaux.

2. Procédure de vote et d'enregistrement des votes exprimés

2.1 Initialisation du bureau de vote

Le matin du jour du scrutin, le président du bureau de vote initialise tous les appareils avant l'ouverture du bureau de vote.

L'initialisation d'un bureau de vote doit être la plus simple possible et nécessiter le moins possible d'opérations.

2.2 Vote proprement dit

Le système doit garantir qu'un électeur ne peut voter qu'une seule fois.

Le système doit reconnaître les différents « types » d'électeurs (par exemple, les électeurs européens qui ne sont pas belges).

Le système doit maintenir le secret du vote en tout temps.

2.3 Vérification du vote

L'électeur doit pouvoir vérifier son vote au moyen de l'impression figurant sur son bulletin de vote. Il doit aussi pouvoir vérifier si son vote peut être lu de manière automatisée en utilisant un scanner dans un isoloir.

2.4 Enregistrement des votes

- **Les votes exprimés sont enregistrés électroniquement. Le résultat est un tableau contenant tous les votes sous forme électronique, qui est stocké sur un support. Des possibilités de back-up sont prévues. L'impression sur les bulletins de vote ne sera lue qu'en cas de doute ou lors de l'exécution d'un audit. Chaque vote est seulement enregistré une fois. Il ne peut être effectué de lien direct ou indirect entre le vote émis et l'identité de l'électeur.**

2.5 Clôture du bureau de vote

À la fin du scrutin, le président clôture le bureau. Il signe les votes enregistrés de manière électronique au moyen de la clef personnelle du bureau de vote (et plus son eID). Il met tous les appareils hors service. Il transmet le support contenant les votes enregistrés au bureau principal.

Toutes les données doivent être ~~sévèrement~~ sérieusement sécurisées.

3. Totalisation des votes

Les possibilités suivantes doivent être prévues :

- **les résultats d'un bureau de vote peuvent être totalisés au niveau cantonal et communal et peuvent ensuite être envoyés vers un système informatique central ;**
- ~~- les résultats d'un bureau de vote peuvent être envoyés directement, sans totalisation, vers un système informatique central ;~~
- **chaque vote est seulement pris en compte une fois lors du recensement.**

~~Le Système informatique central n'entre pas dans le cadre du présent cahier spécial de charges.~~

Prototype de système global (vote + enregistrement + totalisation) compatible avec les standards d'un vote démocratique et les conditions de sécurité non exhaustives décrites ci-après et jointes à titre informatif :

➤ Conditions

Le système doit :

- **être conforme aux dispositions du Conseil de l'Europe (<https://wcd.coe.int/ViewDoc.jsp?id=778189>) ;**
- **garantir le secret du vote. Il ne peut être effectué de lien direct ou indirect entre le vote émis et l'identité de l'électeur ;**
- **assurer un accord parfait entre le choix exprimé et l'enregistrement de celui-ci ;**
- **assurer que tous les votes enregistrés seront bien enregistrés correctement à la clôture du vote, même si des incidents pouvaient se produire au niveau du matériel ou du logiciel ;**
- **garantir qu'un électeur puisse exprimer une seule fois un vote valide ;**
- **être conforme à la législation en matière d'emploi des langues et aux législations électorales ;**

~~Le système ne peut pas émettre de rayonnements susceptibles d'être détectés en dehors de l'isoloir ou du bureau de totalisation.~~

~~Le soumissionnaire fournit tous les appareils et tout le matériel nécessaires à~~

~~l'organisation des élections.~~

~~Les administrations possèdent tous les appareils en nombre suffisant.~~

Les organes suivants doivent pouvoir disposer des appareils adéquats en autant d'exemplaires que nécessaire pour effectuer leur mission :

- Les différentes administrations
- Les organismes de contrôle
- Le Collège des experts

➤ **Fonctionnement**

En cas d'élections simultanées, le système doit clairement faire la distinction entre les différentes élections.

Le bureau de vote doit être à même de traiter minimum 2000 électeurs sur la durée d'ouverture des bureaux de vote (8 h.–15 h.). Doit être clairement précisé ici le nombre de machines qui seront nécessaires pour pouvoir réaliser ceci dans ce laps de temps.

En cas d'anomalie dans le fonctionnement normal à l'intérieur d'un isolement, un système d'alarme doit de préférence en informer le président du bureau.

Tous les PV dans tous les bureaux sont générés selon une procédure simple et sont disponibles sous forme digitale et sous forme d'impression. Ces formats sont liés entre eux de manière à ne devoir signer qu'un seul PV.

Pour toutes les données, une possibilité d'effectuer d'un back-up doit être prévue.

~~La transmission digitale des résultats, accompagnés du PV digital, sera rapide, simple et sécurisée. Un système de back-up sera prévu pour le cas où la transmission digitale venait à échouer.~~

➤ **Votes exprimés**

Le système de vote permet de transférer sur un support de mémoire l'enregistrement des votes exprimés. Le support doit offrir toutes les garanties en termes d'intégrité et de solidité.

Le système :

- **composera par élection, à mesure que les tableaux des votes exprimés transmis par les bureaux de vote seront mis en mémoire, un tableau des résultats par liste et par candidat et suppléant. Le tableau des résultats contiendra tous les votes exprimés dans le canton ou la commune ;**
- **offrira toutes les garanties en termes de confidentialité et de protection de ce tableau, et conservera en permanence au moins une copie des résultats partiels enregistrés;**
- **permettra de diffuser les résultats intermédiaires sans que les bureaux de vote puissent y être identifiés individuellement ;**
- **procédera, pour la mise en mémoire des tableaux des votes exprimés, à des contrôles permettant de s'assurer de l'origine et de l'intégrité de chaque tableau. Chaque tableau provenant d'un bureau de vote ne sera pris en compte qu'une seule fois ;**
- **permettra de vérifier si le nombre de bulletins de vote mis en mémoire correspond au nombre d'électeurs qui se sont présentés dans le bureau de vote ;**
- **offrira la possibilité de recompter manuellement un bureau de vote sur la base de l'information textuelle du bulletin de vote ;**
- ~~n'aura pas besoin de plus de 5 secondes pour intégrer dans le système de totalisation le tableau des votes exprimés se trouvant sur un support de mémoire provenant d'un bureau de vote.~~

- ~~Intégration par le prototype de vote de la possibilité d'adjonction d'accessoires techniques dans le cadre d'un vote facilité pour les personnes malvoyantes.~~
- ~~Fourniture avec le prototype de vote d'une documentation claire et détaillée. Cette documentation fera l'objet d'une évaluation de la part du pouvoir adjudicateur qui se réservera le droit de demander des améliorations et des modifications à celle-ci.~~
- ~~Fourniture avec le prototype de vote du know-how et de l'estimation des ressources nécessaires à sa maintenance.~~

Annexe E – Rapport d'évaluation du code-source avec l'outil Sonar

Nous renvoyons à ce propos au document « Onderzoek van de broncode van het prototype van bevoiting via de Sonar tool met PWC.pdf », joint à la version électronique de ce rapport.

Annexe F – Rapports d’observation détaillés (ROD)



Rapport d'observation		Référence :	ROD-001
		Statut :	
Constat d'observation :	La redondance des données sur la clef USB Master concernant les fichiers election.xml peut encore être diminuée.		
Description			
Observé par :	Sander Van der Meulen	Date de l'observation :	13 December 2011
Contact :	sander.van.der.meulen@pwc.be		
Niveau d'importance :	B - demande une réponse/solution avant la fin de l'évaluation		
Module :	PREP Préparation		
Activité au cours de laquelle l'observation a été faite :	Pendant la vérification du contenu de la clef USB Master après sa création.		
Description détaillée de l'observation :	<p>La mise en oeuvre du prototype du système n'est pas conforme aux critères d'acceptation (CusIssPr174). Nous avons observé que le fichier election.xml n'est pas unique par clef USB Master. Pour les élections fédérales (2010), nous avons trouvé plusieurs fichiers election.xml, plus précisément 1 par commune (ce qui a été constaté spécifiquement pour la commune avec des divisions communales Anvers, la commune de Brecht et la commune d'Alost). Etant donné que la circonscription électorale se situe au niveau provincial pour les élections à la Chambre, cela démontre que le fichier n'est pas toujours établi au niveau le plus bas des circonscriptions électorales de l'élection pour laquelle la clef USB est faite, comme précisé dans les critères d'acceptation (sauf pour les élections communales). Il ne peut y avoir qu'un seul fichier election.xml par province comprenant les informations relatives à la Chambre et au Sénat. Ceci devrait veiller à ce que chaque fichier election.xml soit unique par combinaison unique d'élections : Chambre, province X et Sénat. Concrètement la commune avec des divisions communales Anvers ou la commune de Brecht ne devraient pas contenir chacune un fichier election.xml. Etant donné que c'est cependant bien le cas, il y a plusieurs copies identiques de ce fichier sur la clef USB Master, ce qui témoigne d'une redondance de données.</p>		
Renvoi vers du matériel probant			
Analyse d'impact			
Analyse d'impact :	Pas de grand impact. Cependant, la performance du processus de création de la clef USB Master peut probablement être accrue si les données superflues ne doivent pas être créées (et copiées) sur les clefs USB.		
Recommandation			
Solution proposée :	Créer le fichier election.xml au niveau le plus bas de la circonscription électorale applicable pour l'élection en question plutôt qu'au niveau communal pour chaque élection.		
Résultat final			
Résultat final :	Lors de la réunion du 24 novembre 2011 où les représentants des divers pouvoirs étaient présents, il a été confirmé en présence de PwC que la mise en oeuvre était OK telle qu'elle s'était déjà déroulée à ce moment. Les représentants étaient conscients que d'autres améliorations devaient encore être apportées pour encore réduire la redondance. Il y a eu un accord pour que cela puisse être effectué après la livraison du prototype. Une réduction significative de la redondance avait cependant déjà été constatée, ce qui est déjà une évolution très positive.		
Risque subsistant			
Estimation du risque subsistant après la réponse / la solution de Steria-Smartmatic	Aucun, étant donné que cette observation n'a pas d'impact sur les fonctionnalités de base du processus de vote. L'observation constatée n'a d'impact que sur l'efficacité du processus de préparation.		



Rapport d'observation		Référence :	ROD-002
		Statut :	
Constat d'observation :	Il n'y a pas de fichiers PDF des écrans de dialogue créés pendant la création des écrans sur l'application ECM		
Description			
Observé par :	Sander Van der Meulen	Date de l'observation :	09 December 2011
Contact :	sander.van.der.meulen@pwc.be		
Niveau d'importance :	B - demande une réponse/solution avant la fin de l'évaluation		
Module :	PREP Préparation		
Activité au cours de laquelle l'observation a été faite :	Vérification de l'export en PDF après le traitement des écrans sur l'application ECM		
Description détaillée de l'observation :	La mise en oeuvre du prototype du système n'est pas conforme aux critères d'acceptation (CusIssPr167). Après le traitement des écrans générés sur l'application ECM des 3 communes pour les élections fédérales (2009), nous les avons exportés vers une clef USB en format FAT32. Lors de l'ouverture du fichier screenshots.zip sur un PC sous Windows, nous avons constaté que des fichiers PDF avaient bien été créés au niveau de la circonscription électorale telle que décrite dans les critères d'acceptation. Cependant, ces fichiers PDF ne contiennent que 1 ou 2 aperçu(s) (resp. Chambre et Sénat) et liste(s) de candidats (du premier parti sur l'aperçu du parti). Les écrans de dialogue n'étaient pas présents dans les fichiers PDF, ce qui n'est pas conforme aux critères d'acceptation.		
Renvoi vers du matériel probant	OBR-002_Chamber.pdf OBR-002_Senate.pdf		
Analyse d'impact			
Analyse d'impact :	Pas de grand impact. L'utilisateur a toujours la possibilité d'imprimer les fichiers .png des écrans de dialogue. Cependant ces fichiers sont générés sur une clef USB en format EXT3 et ne sont donc pas lisibles sur un PC sous Windows, ce qui rend ce processus non convivial.		
Recommandation			
Solution proposée :	Traiter aussi les écrans de dialogue lors du traitement des écrans sur l'application ECM, de sorte que ceux-ci soient également traités dans les fichiers PDF.		
Résultat final			
Résultat final :	Cette erreur a été reconnue par Smartmatic et sera ajoutée à la liste des points en suspens. Cela peut être résolu en corrigeant un paramètre dans la configuration.		
Risque subsistant			
Estimation du risque subsistant après la réponse / la solution de Steria-Smartmatic	Le problème est facile à résoudre et ne résulte pas en un risque subsistant.		

1 VLAAMS BELANG	9 CDV	13 GROEN!	25 RESPECT
3 LIJST DEDECKER	10 sp·a	15 LSP	Blanco stem
4 open vld	11 N-VA	19 pvd+	

Selecteer een lijst of stem blanco

KAMER VAN VOLKSVERTEGENWOORDIGERS

1  **VLAAMS
BELANG**

1 D'HAESELEER
Guy

2 PAS
Barbara

3 VEYS
Tanguy

4 HERMAN
Steve

5 DESSEIN
Sabrina

6 WOLF
Frauke

7 BOURLAU
Stephan

8 EVRARD
Olaf

9 TRUYMAN
Toon

10 WAUTERS
Mia

11 VAN BOVEN
Lena

12 CREYELMAN
Steven

13 SEGERS
Patricia

14 BRACKE
Wouter

15 CRAESSAERTS
Ilse

16 LIEVENS
Jan

17 DE BOEVER
Gabi

18 ROMBAUT
Sylvia

19 DE GUSSEM
Veerle

20 WYMEERSCH
Frans

Opvolgers

1 CLEYMAN
Alain

2 VAN STEENBERGE
Gerda

3 DEPOORTERE
Ortwin

4 SLAGMULDER
Kristof

5 REYNIERS
Marleen

6 DE ROO
Patrick

7 VAN MOESEKE
Heidrun

8 WALLAERT
Bart

9 MATHYS
Marie-Jeanne

10 GEERS
Gilberte

11 TACK
Erik

Keer terug naar het vorige scherm

1 **VLAAMS
BELANG**

9 **CDV**

13 **ERGOEN!**

19 **pvd+**

3 **LIJST
DEDECKER**

10 **sp·a**

15 **LSP**

Vote Blanc

4 **open vld**

11 **N-VA**

17 **CHP**

Sélectionnez une liste ou votez blanc

1  **VLAAMS
BELANG**

1 DEWINTER

Filip

23 DE LOBEL

Hilde

2 VAN DERMEERSCH

Anke

24 VAN GAEVER

Freddy

3 CEDER

Jurgen

25 COVELIERS

Hugo

4 JANSEGERS

Nele

5 VAN OVERMEIRE

Karim

6 VISSERS

Linda

7 CREYELMAN

Frank

8 LAEREMANS

Jan

9 BRAEM

An

10 PEETERS - MUYSHONDT

Annemie

11 OOMS

Koen

12 BONTE

Barbara

13 VAN DIJCK

Wim

14 DECKMYN

Johan

15 WIENEN

Wim

16 WARPY

Sonja

17 TOURNOIJ

Katty

18 RAMAN

Hilde

19 SMETS

Geert

20 HEYLEN

Christel

21 DURNEZ

Patsy

22 INDEHERBERGE

Karel

Suppléant

1 BUYSSE

Yves

2 JANSEGERS

Nele

3 ERENS

Frédéric

4 SOMERS

Werner

5 VAN ECHELPOEL

Hilde

6 VAN HAELST

Goedele

7 DOUCET

Veronique

8 PANNECOUCKE

Roland

9 PAUWELS

Peter

10 DECANNIERE

Martine

11 VAN BEUGHEM

Nadia

12 VLAMINCK

Etienne

13 DE MEY

Reddy


14 DILLEN

Marijke

Revenez à l'écran précédent

1 VLAAMS BELANG	9 CDV	13 ERGOEN!	19 pvd+
3 LIJST DEDECKER	10 sp·a	15 LSP	Blanco stem
4 open vld	11 N-VA	17 CHP	

Selecteer een lijst of stem blanco

1  VLAAMS BELANG			
1	DEWINTER Filip	23	DE LOBEL Hilde
2	VAN DERMEERSCH Anke	24	VAN GAEVER Freddy
3	CEDER Jurgen	25	COVELIERS Hugo
4	JANSEGERS Nele		
5	VAN OVERMEIRE Karim		
6	VISSERS Linda		
7	CREYELMAN Frank		
8	LAEREMANS Jan		
9	BRAEM An		
10	PEETERS - MUYSHONDT Annemie		
11	OOMS Koen		
12	BONTE Barbara		
13	VAN DIJCK Wim		
14	DECKMYN Johan		
15	WIENEN Wim		
16	WARPY Sonja		
17	TOURNOIJ Katty		
18	RAMAN Hilde		
19	SMETS Geert		
20	HEYLEN Christel		
21	DURNEZ Patsy		
22	INDEHERBERGE Karel		
		Opvolgers	
		1	BUYSSE Yves
		2	JANSEGERS Nele
		3	ERENS Frédéric
		4	SOMERS Werner
		5	VAN ECHELPOEL Hilde
		6	VAN HAELST Goedele
		7	DOUCET Veronique
		8	PANNECOUCKE Roland
		9	PAUWELS Peter
		10	DECANNIERE Martine
		11	VAN BEUGHEM Nadia
		12	VLAMINCK Etienne
		13	DE MEY Reddy
		14	DILLEN Marijke

Keer terug naar het vorige scherm



Rapport d'observation		Référence :	ROD-003
		Statut :	
Constat d'observation :	Il n'y a pas de "log" convivial présent des modifications apportées via la fonctionnalité "change candidate names".		
Description			
Observé par :	Sander Van der Meulen	Date de l'observation :	09 December 2011
Contact :	sander.van.der.meulen@pwc.be		
Niveau d'importance :	B - demande une réponse/solution avant la fin de l'évaluation		
Module :	PREP Préparation		
Activité au cours de laquelle l'observation a été faite :	L'exécution de tests concernant la fonctionnalité "change candidate names" dans l'application ECM.		
Description détaillée de l'observation :	<p>La mise en oeuvre du prototype du système n'est pas conforme aux critères d'acceptation (CusIssPr193). Au cours des tests de la fonctionnalité "change candidate names", nous avons constaté qu'il n'était pas conservé de "log" dans l'application ECM, des modifications qui sont apportées aux noms des candidats et des listes.</p> <p>Un "log" est bien conservé sur le serveur, à savoir le fichier smmt.log dans la directory /opt/ecm/conf/logs. Pour trouver ce fichier, il faut cependant utiliser un terminal, en quittant l'application. Ce fichier "log" contient d'ailleurs un aperçu de toutes les activités sur le système de préparation, ce qui peut fournir rapidement quelques milliers de lignes. De ce fait, l'activité liée à la modification des noms des candidats ou des partis est très difficile à tracer. Cette méthode de travail est à notre avis non conviviale et ne correspond pas aux attentes du pouvoir adjudicateur.</p>		
Renvoi vers du matériel probant			
Analyse d'impact			
Analyse d'impact :	Pas de grand impact. La phase de préparation se déroule dans un environnement contrôlé. La conservation d'un rapport "log" pourrait être un contrôle supplémentaire qui détecte l'absence de login et de mot de passe lors de cette fonctionnalité.		
Recommandation			
Solution proposée :	Mise en oeuvre d'un rapport de "log" simple pour cette fonctionnalité, de sorte qu'on puisse vérifier par la suite qui a effectué quelles modifications. En outre, ce rapport peut servir de base pour effectuer aussi les modifications apportées dans l'application des candidats.		
Résultat final			
Résultat final :	Smartmatic va créer un "user log" avec des marques de temps et une indication "avant" et "après" pour les modifications. Ce "log" ne comprendra que des informations sur ces modifications.		
Risque subsistant			
Estimation du risque subsistant après la réponse / la solution de Steria-Smartmatic	Faible, étant donné que cela n'a pas d'impact direct sur les résultats du vote eux-mêmes. Les informations nécessaires sont présentes, mais ne sont pas accessibles de manière suffisamment conviviale.		



Rapport d'observation		Référence :	ROD-004
		Statut :	
Constat d'observation :	Les tests de diagnostic ne sont pas tout à fait conformes aux critères d'acceptation.		
Description			
Observé par :	PwC	Date de l'observation :	15 December 2011
Contact :	mathieu.ghys@pwc.be		
Niveau d'importance :	B - demande une réponse/solution avant la fin de l'évaluation		
Module :	Général		
Activité au cours de laquelle l'observation a été faite :	Au cours de l'exécution des tests de diagnostic sur la machine du président, la machine de vote et le système de totalisation. Pour les machines de vote et du président, il s'agit ici des tests du menu de maintenance et des tests qui peuvent être effectués à l'avance à l'aide de la clef USB "diagnose-only". Pour le système de totalisation, il s'agit des tests qui doivent être effectués au démarrage de l'application et qui sont réexécutables via la "tab" 'Diagnose'.		
Description détaillée de l'observation :	<p>Les observations ne sont pas conformes aux critères d'acceptation (CusIssP280, CusIss076, CusIss134, CusIss233, CussIssT016).</p> <p>Nous avons observé que les tests de diagnostic réalisés sur la machine du président s'écartaient plusieurs fois des critères d'acceptation :</p> <ul style="list-style-type: none"> - En cas d'échec du test de l'imprimante, du lecteur de smartcard et de la clef USB, aucune solution n'est proposée (sauf pour le diagnostic individuel de l'imprimante lorsque celle-ci n'est pas connectée à la machine du président). Les tests des lecteurs de codes-barres prévoient alors une solution pour reconfigurer le lecteur avec une série de codes-barres, mais uniquement dans le test de diagnostic individuel. En outre pendant le diagnostic du lecteur de codes-barres, il n'est pas fait mention d'un manque d'encre ou de papier dans l'imprimante. Le test de la clef USB "diagnose-only" échoue en outre toujours. Ce n'est que lorsqu'on introduit une clef USB formatée (à côté de la clef USB "diagnose-only"), que le test réussit. - Quelques "crashes" de la machine du président ont aussi été constatés lorsque l'imprimante est déconnectée et ensuite reconnectée. <p>D'autre part, les tests de diagnostic de la machine de vote présentent d'autres défauts :</p> <ul style="list-style-type: none"> - Ainsi, aucune solution n'est proposée, sauf en cas de diagnostic individuel du lecteur de codes-barres, du test de calibrage et de la netteté de l'écran. - La machine de vote ne signale aucune erreur lorsque le papier de l'imprimante est presque vide. Lorsque le papier est vide, l'erreur signalée est que le papier est vide ou presque vide. Enfin, lors du démarrage de la fonctionnalité "diagnose-only", il n'est pas indiqué ce que l'utilisateur doit faire. <p>Enfin, les résultats du test de diagnostic du système de totalisation ne correspondent pas totalement aux critères d'acceptation, à cause du défaut suivant :</p> <ul style="list-style-type: none"> - L'absence d'imprimante n'est pas toujours détectée lors d'une opération d'impression et le système continue à essayer de se connecter à l'imprimante (nous avons attendu ici pendant 5 minutes). 		
Renvoi vers du matériel probant	OBR-004_evidence.pdf		
Analyse d'impact			
Analyse d'impact :	Pas de grand impact sur le cours effectif des élections et la totalisation. Cette problématique peut cependant jouer un rôle lors de l'exécution des tests de diagnostic dans le magasin ou le bureau de vote lors de la préparation des élections. Cela a aussi un impact possible sur l'exécution du test de diagnostic dans un bureau de totalisation lors de la préparation de la totalisation.		
Recommandation			
Solution proposée :	Etablir les critères d'acceptation définitifs par Smartmatic en collaboration avec le SPF Intérieur, et se mettre d'accord sur les tests de diagnostic sur ces critères.		
Résultat final			
Résultat final :	<p>Les tests sur les machines du président/machines de vote seront réexaminés pour tenir compte des observations ci-dessus.</p> <p>La clef "Diagnose only USB" sera encore retravaillée et complétée, avec notamment un fichier/rapport de "log" par machine testée.</p> <p>Voir également la réunion du 24/10 entre Smartmatic et le groupe de travail, où il a été confirmé que les modifications à et l'optimisation des tests de diagnostic ont pu continuer à être réalisées aussi après le 30/11.</p>		
Risque subsistant			
Estimation du risque subsistant après la réponse / la solution de Steria-Smartmatic	Des tests corrects de diagnostic réalisables et fiables, où des informations claires sont rendues disponibles sur les tests réalisés et leurs résultats, réduisent le risque sur des défauts évitables du matériel le jour des élections, ce qui peut éviter une perte de temps (par exemple en remplaçant le matériel).		

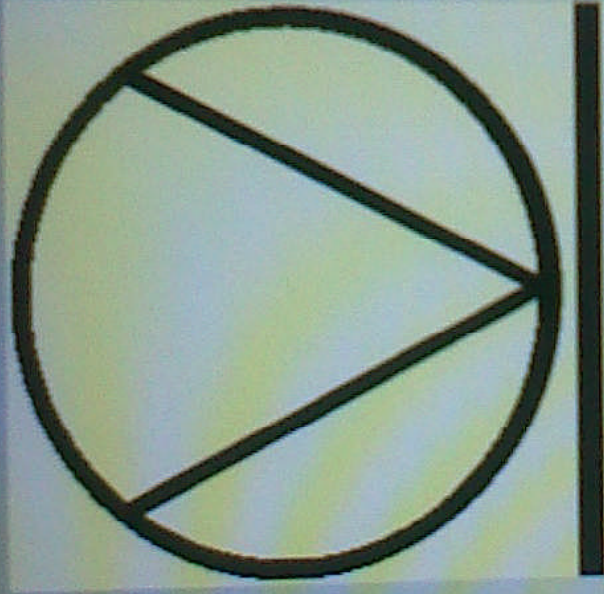


Erreur d'imprimante: Plus de papier
Erreur d'imprimante: Fin imminente du papier

Erreur

Ok

Diagnose volledig systeem

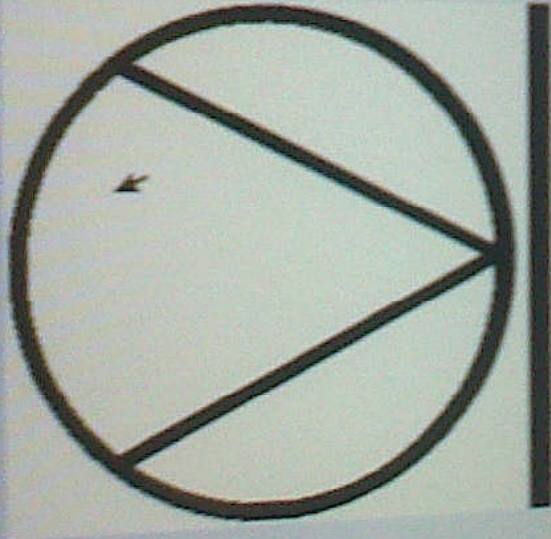


A

Fout afdrukeenheid: Buiten dienst

Fout

OK



De printer kan niet worden gedetecteerd. Verzeker er u van dat de printer is aangesloten en herstart de voorzittersmachine. Indien de fout zich blijft voordoen, gelieve om technische bijstand te vragen.

Fout

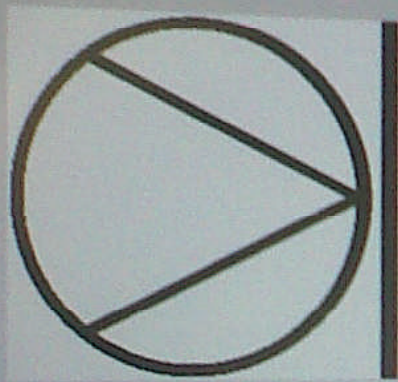
OK

Diagnose volledig systeem



Kan de barcodelezer niet bereiken. Diagnose is mislukt

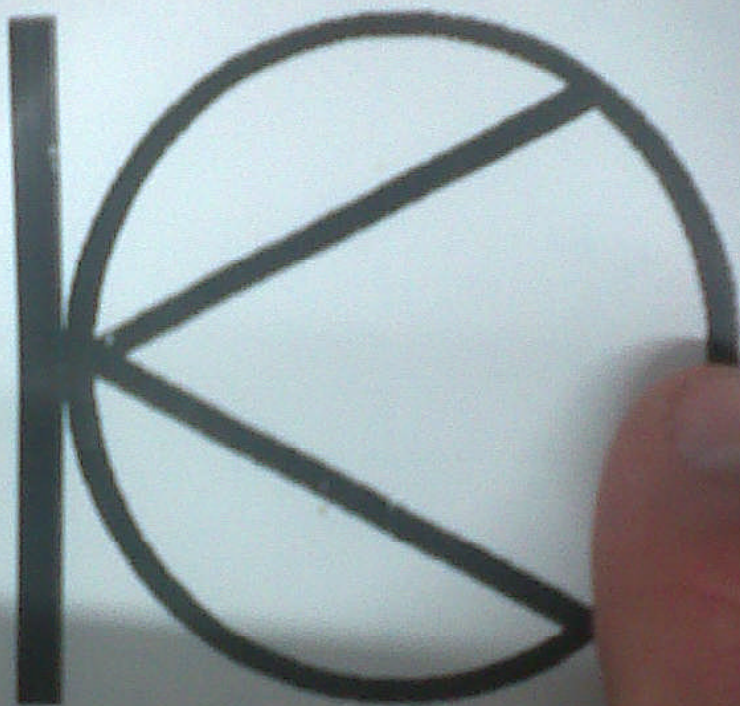
Het apparaat BARCODELEZER werd niet
gedecteerd. Gelieve correct aan te sluiten.
Als de fout aanhoudt, vraag om technische bijstand



Fout afdrukeenheid: Papier zit klem
Fout afdrukeenheid: Printpapier bijna op

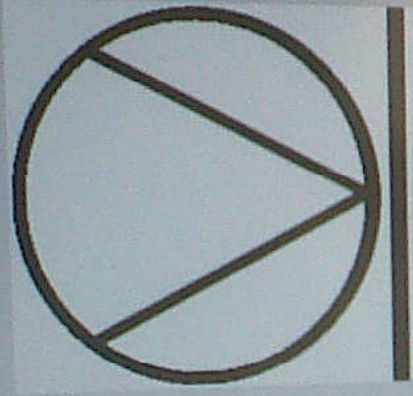
Fout

OK



Diagnose d

Diagnose drukker



Diagnose drukker geslaagd

Fout

OK



Alarmdoos is niet bereikt. Diagnose mislukt

Het apparaat BARCODELEZER werd niet
gedecteerd. Gelieve correct aan te sluiten.
Als de fout aanhoudt, vraag om technische bijstan

Kan de barcodelezer niet bereiken. Diagnose is mislukt



Rapport d'observation		Référence :	ROD - 005
		Statut :	
Constat d'observation :	L'application RTS n'est pas toujours stable dans un usage normal.		
Description			
Observé par :	Jeffrey Beetens	Date de l'observation :	15 December 2011
Contact :	jeffrey.beetens@pwc.be		
Niveau d'importance :	B - demande une réponse/solution avant la fin de l'évaluation		
Module :	TOT Totalisation		
Activité au cours de laquelle l'observation a été faite :	Au cours de l'exécution et des tests de l'ensemble du processus de totalisation.		
Description détaillée de l'observation :	<p>L'application n'est pas toujours apparue stable au cours de son utilisation. Les exemples suivants étayent cette conclusion :</p> <ul style="list-style-type: none"> - Lorsqu'on tente de démarrer le système en mode 'recovery', il est apparu que cette option n'était pas toujours présente alors que des back-ups avaient déjà été faits avec des bureaux de vote totalisés. Il n'était plus possible de se "logger" au bureau de totalisation de Saint-Gilles pour les élections européennes, régionales, pour la Chambre & le Sénat. Néanmoins, après la cinquième réinstallation, le mode 'recovery' est réapparu à nouveau et il fut possible de poursuivre jusqu'à l'écran où les tests de diagnostic doivent être effectués. Lorsqu'on a continué ensuite, est apparu un message d'erreur qui indiquait qu'un problème inattendu s'était produit. Après le redémarrage du système, on a finalement pu continuer à travailler correctement. - Parfois le 'mouse pad' s'est bloqué après la modification de la date et de l'heure. Ce n'est qu'après avoir appuyé sur 'tab' qu'on a pu continuer à travailler normalement. Néanmoins, lorsqu'on utilise la souris, on peut travailler sans problème. - Dans un seul cas (pour les élections provinciales et communales dans les Fourons) deux boutons sont apparus, à savoir 'Suivant' et 'Terminer' après la totalisation des résultats du dernier bureau de vote. Si on choisissait 'Terminer', le système affichait à nouveau l'écran pour totaliser plus de clefs USB, alors que dans tous les autres cas (où le bouton 'Suivant' était donc disponible) apparaissait directement l'écran d'aperçu et plus aucune clef USB ne pouvait être totalisée. - Dans certains cas le système de totalisation ne pouvait plus imprimer de documents. Ce n'est qu'en redémarrant le système que tous les documents qui se trouvaient dans la file d'attente pouvaient être imprimés. 		
Renvoi vers du matériel probant	OBR_005_evidence.pdf		
Analyse d'impact			
Analyse d'impact :	Pas de grand impact. Cependant, la performance du processus de totalisation peut être améliorée s'il n'est pas nécessaire de redémarrer plusieurs fois le système, de le réinstaller et/ou d'entreprendre d'autres actions.		
Recommandation			
Solution proposée :			
Résultat final			
Résultat final :	Smartmatic continuera à effectuer des tests et réalisera des QA complémentaire pour résoudre les problèmes ci-dessus.		
Risque subsistant			
Estimation du risque subsistant après la réponse / la solution de Steria-Smartmatic	Si les problèmes de stabilité ne peuvent être résolus suffisamment ou complètement, il subsiste le risque de perte de temps lors de la totalisation.		

Analysen
Diagnose
Verslagen

Totalisatie

[IP-adres: 192.168.56.2 | MAC-adres: 78-2B-CB-CC-05-19]

Geavanceerd van totalisation
[VOEREN : Voeruitgang totalisatie]
5 van 5

Volledig aantal stembureaus verwerkt

De totalisatie werd met succes afgerond. U kunt de geheugendragers verwijderen.

Resultaat per verkiezingsbureau

VOEREN-003	
Gemeenteraad Voeren	Verwerking OK
OCMW raad Voeren	Verwerking OK
Provincieraad Tongeren	Verwerking OK

Volgende Finish

Check

Totalisatie

[IP-adres: 192.168.56.2 | MAC-adres: 78-2B-CB-CC-05-19]

[VOEREN : Vooruitgang totalisatie]

5 van 5

100,00%

Volledig aantal stembureaus verwerkt

Druk op de knop 'Afsluiten totalisatie' om verder te gaan

Verwerkt USB-geheugendragers

Afsluiten totalisatie

Gegevens exporteren

Apparaat uitschakelen

Plaats één of meerdere geheugendragers



Volgende



Er heeft zich een onverwachte fout voorgedaan / Une erreur inattendue s'est produite





Rapport d'observation		Référence :	ROD-006
		Statut :	
Constat d'observation :	Lorsqu'on retire la clef USB 'Master', cela ne s'indique pas sur les PC 'esclaves' du même réseau.		
Description			
Observé par :	Jeffrey Beetens	Date de l'observation :	05 December 2011
Contact :	jeffrey.beetens@pwc.be		
Niveau d'importance :			
Module :	TOT Totalisation		
Activité au cours de laquelle l'observation a été faite :	Lors du retrait de la clef USB 'Master' dans un réseau de totalisation.		
Description détaillée de l'observation :	<p>Bien que nous conseillions que la clef USB de back-up soit toujours présente au cours du processus de totalisation, il a été décidé de commun accord entre SmartMatic et le SPF Intérieur que ce n'était pas nécessaire à condition qu'un message apparaisse sur le PC master et les PC 'esclaves' (voir le rapport de la réunion du 24/11 où on peut lire la conclusion suivante : <i>"L'administration accepte que si le backup (USB) tombe en panne pendant la totalisation, apparaît un message qu'on peut faire disparaître via le bouton "ESC". Toutes les 6 secondes (paramétrisables) un message de rappel apparaît jusqu'à ce qu'un nouveau backup soit présent."</i></p> <p>Pour le moment cette mention (qu'on peut faire disparaître via le bouton "ESC" et un rappel toutes les 6 secondes) apparaît en effet sur le PC master, mais pas sur les PC 'esclaves' dans le réseau configuré.</p>		
Renvoi vers du matériel probant			
Analyse d'impact			
Analyse d'impact :	En cas d'absence de l'utilisateur du PC master, les utilisateurs des PC 'esclaves' ne sont pas informés du fait que la clef USB de back-up n'est pas présente, ce qui peut conduire à la perte des résultats de totalisation en cas de crash du système de totalisation et par conséquent à une perte de temps, du fait que le processus de totalisation doit à nouveau être exécuté après la réinstallation (même via le mode 'recovery').		
Recommandation			
Solution proposée :	Réaliser les fonctionnalités telles que convenues dans les critères d'acceptation.		
Résultat final			
Résultat final :	Le message sur le PC 'esclave' en cas de retrait de la clef USB 'Master' sera développé.		
Risque subsistant			
Estimation du risque subsistant après la réponse / la solution de Steria-Smartmatic	Le problème est facile à résoudre et ne résulte pas en un risque subsistant.		



Rapport d'observation		Référence :	ROD-007
		Statut :	
Constat d'observation : Il n'y a pas de confirmation obligatoire de la date et de l'heure après s'être connecté dans l'application RTS.			
Description			
Observé par :	Jeffrey Beetens	Date de l'observation :	07 December 2011
Contact :	jeffrey.beetens@pwc.be		
Niveau d'importance :	B - demande une réponse/solution avant la fin de l'évaluation		
Module :	TOT Totalisation		
Activité au cours de laquelle l'observation a été faite :	L'écran d'aperçu (avec les différents boutons pour les tests de diagnostic et la date et l'heure) après s'être "loggé" dans l'application RTS.		
Description détaillée de l'observation :	<p>La confirmation de la date et de l'heure après s'être "loggé" dans l'application RTS n'est pas une étape obligatoire de sorte que le problème suivant peut survenir :</p> <ul style="list-style-type: none"> - Les back-ups ne sont faits que si la date-système (telle que configurée dans l'application RTS) est plus récente que celle du dernier back-up. Cela signifie que si la date est introduite de manière inexacte à l'avenir et n'est remplacée qu'après 3 périodes de back-up selon la date propre telle qu'initialement configurée, plus aucun nouveau back-up ne peut être réalisé. 		
Renvoi vers du matériel probant			
Analyse d'impact			
Analyse d'impact :	Il est possible que des back-ups avec de nouveaux résultats ne puissent plus être enregistrés, ce qui peut conduire en cas de crash du système de totalisation à la perte des résultats de totalisation et par conséquent à une perte de temps du fait que l'ensemble du processus de totalisation doive à nouveau être exécuté après la réinstallation (même via le mode 'recovery').		
Recommandation			
Solution proposée :	Rendre obligatoire de corriger la date et l'heure lors du démarrage du système de totalisation.		
Résultat final			
Résultat final :	Le problème sera ajouté à Jira et la confirmation obligatoire de la date et de l'heure au démarrage du système de totalisation sera mise en place.		
Risque subsistant			
Estimation du risque subsistant après la réponse / la solution de Steria-Smartmatic	Si la confirmation de la date et de l'heure est correctement mise en place lors du démarrage du système de totalisation, le risque disparaît que les back-ups ne soient pas faits à cause d'une erreur de date ou d'heure.		



Rapport d'observation		Référence :	ROD - 008
		Statut :	
Constat d'observation :	Les procès-verbaux et les fichiers de résultats exportés au niveau de la totalisation contiennent encore des erreurs.		
Description			
Observé par :	Loic D'Haeyer	Date de l'observation :	
Contact :	loic.dhaeyer@pwc.be		
Niveau d'importance :	B - demande une réponse/solution avant la fin de l'évaluation		
Module :	TOT Totalisation		
Activité au cours de laquelle l'observation a été faite :	Pendant l'examen des fichiers exportés, à savoir les fichiers CODI, des PV et des annexes.		
Description détaillée de l'observation :	<p>Pendant l'évaluation des fichiers CODI exportés, nous avons observé les erreurs suivantes :</p> <p>Remarques générales par rapport aux PV :</p> <ol style="list-style-type: none"> (1) L'absence du nombre de votes enregistrés et de votes blancs (2) Le positionnement erroné de la signature électronique, ce qui peut rendre certaines informations illisibles sur le PV (3) L'usage incorrect des extensions _NL et _FR dans les noms de fichiers .pdf (4) L'usage erroné du modèle AB25B-bis (5) L'absence de somme de contrôle sur le PV <p>Remarques générales par rapport aux fichiers de résultats (fichiers X7S et fichiers CODI finaux)</p> <ol style="list-style-type: none"> (6) L'usage de sets incorrects de caractères pour les partis et les candidats, a conduit à une interprétation erronée du caractère "é" et l'apparition du caractère "?" dans les noms (par exemple : Damien Thi?ry). (7) Si les noms des listes, des candidats et des alias ne correspondent pas au fichier CODI initial, cela crée des problèmes lors du chargement de ces fichiers de résultats dans l'environnement CODI. (8) Les extensions _NL et _FR pour les territoires bilingues manquent et il n'y a toujours qu'un seul fichier, alors qu'il en faut deux. (9) La dénomination des fichiers CODI finaux n'est pas toujours correcte : par exemple CSnnnnn.DI au lieu de DMnnnnn.DI pour les conseils de district communaux, <p>Remarques spécifiques par rapport aux fichiers de résultats pour des élections spécifiques :</p> <p>Chambre et Sénat :</p> <ol style="list-style-type: none"> (10) Les noms des candidats sont en caractères d'imprimerie, alors qu'ils doivent être indiqués tels qu'ils sont mentionnés dans le Registre de la population (c'est-à-dire que toutes les lettres ne sont pas des caractères d'imprimerie). (11) Bien que ceci ne soit pas un champ obligatoire, nous avons observé que la langue du collège électoral était défini erronément comme "NF". <p>Parlement européen et régionaux :</p> <ol style="list-style-type: none"> (12) Le nombre de votes enregistrés n'est pas correct : ce doit être la somme des deux collèges. (13) La langue du collège électoral est mentionnée pour le parlement flamand, alors que ce n'est pas nécessaire. (14) Les listes ne sont pas triées correctement : d'abord par collège et ensuite par numéro de liste alors qu'elles doivent uniquement être triées par numéro de liste. (15) Nous avons observé que l'extension du fichier CODI pour les membres bruxellois du parlement flamand n'est pas correcte. Le fichier a reçu par erreur l'extension "VL" au lieu de "BV". (16) Le type du bureau de clôture n'est pas correct (C au lieu de R), <p>Elections locales (Communes / Provinces / CPAS / District) :</p> <ol style="list-style-type: none"> (17) L'ordre de dépôt n'est pas conforme au "Format F" (des chiffres au lieu de lettres). 		
Renvoi vers du matériel probant	Rapport de réunion du groupe de travail		
Analyse d'impact			
Analyse d'impact :	<p>Au cours d'une réunion du groupe de travail du 19/12/2011, il a été décidé qu'aucun procès-verbal ne doit plus être généré au niveau de la totalisation, ce qui fait tomber les remarques ci-dessus concernant les PV. Il s'agit des remarques (1) à (5). En outre, nous reconnaissons qu'en ce qui concerne le problème (7), Stésud avait confirmé à plusieurs reprises (à Smartmatic en présence du gouvernement) que la modification des noms des candidats n'avait pas d'influence sur le fonctionnement du système. Or, aujourd'hui, les problèmes lors du chargement des fichiers de résultats sont bien à attribuer à la modification des noms de candidats. Enfin, nous précisons que les autres remarques sont dues à un manque de spécifications claires du format CODI.</p> <p>Si les fichiers exportés ne répondent pas au standard (Format F), il y a un risque que les résultats ne puissent être mémorisés au niveau suivant. Etant donné (a) que CODI n'était pas encore utilisé lors des élections locales précédentes en 2006 et que les spécifications pour les élections concernées et les fichiers n'étaient pas clairement décrites et (b) que lors des élections locales de 2012, la Flandre n'utilisera pas le système de totalisation, mais que les résultats seront directement chargés de la machine du président dans l'environnement CODI via une interface qui doit encore être développée et (c) que le système de totalisation lors des prochaines élections locales à Bruxelles ne sera mis en oeuvre que dans deux communes bruxelloises et (d) que les points laissés en suspens peuvent être résolus dans un délai raisonnable, nous considérons ce point comme 'non bloquant'.</p>		
Recommandation			
Solution proposée :	La condition pour que Smartmatic puisse résoudre les points en suspens dans un délai raisonnable est de disposer des spécifications concrètes/détaillées du format CODI.		
Résultat final			
Résultat final :	Smartmatic ne peut résoudre les problèmes liés aux spécifications du format CODI (entre autres les remarques 3, 7, 8, 9 et 15) que si le gouvernement met à la disposition de Smartmatic les spécifications claires et <u>complètes</u> fournies par Stésud. Les problèmes qui ne sont pas liés aux spécifications du format CODI continueront à être examinés et si c'est pertinent seront résolus.		
Risque subsistant			
Estimation du risque subsistant après la réponse / la solution de Steria-Smartmatic	Si les fichiers de résultats ne sont pas totalement conformes aux spécifications du format CODI, le risque subsiste de ne pouvoir mémoriser ces fichiers.		



Rapport d'observation		Référence :	ROD-009
		Statut :	
Constat d'observation :	Le hardware a présenté parfois un comportement instable pendant l'exécution des plans de test.		
Description			
Observé par :	PwC	Date de l'observation :	19 December 2011
Contact :	mathieu.ghys@pwc.be		
Niveau d'importance :			
Module :	Général		
Activité au cours de laquelle l'observation a été faite :	Les observations concernant l'instabilité du hardware ont été faites pendant l'exécution de tests dans les phases de préparation et de vote.		
Description détaillée de l'observation :	<p>Au total, quatre problèmes de hardware ont été constatés :</p> <ol style="list-style-type: none"> 1. Lors du formatage des nouvelles clefs USB fournies (reçues le 30/11/2011) au moyen du duplicateur Kanguru, on a observé un niveau élevé d'échecs (environ 80%), ce qui signifie concrètement que 4 clefs USB sur 5 ne pouvaient être formatées correctement. Mais le formatage des clefs USB récemment fournies (reçues le 13/12/2011) au moyen du duplicateur Kanguru se déroule bien. 2. L'imprimante connectée au système ECM n'était plus reconnue par le système. On ne pouvait plus rien imprimer pendant la phase de préparation. Le problème n'a pas pu être résolu via la configuration du système. Après une réinstallation du logiciel ECM, le problème a été résolu et on a à nouveau pu imprimer. Ce problème n'a pas pu être reproduit par la suite. 3. Le lecteur de smartcard de la machine de vote est tombé deux fois en panne. Chaque fois le message est apparu que la smartcard était mal introduite, parfois même quand aucune smartcard n'était introduite. Le test de diagnostic du lecteur indiquait aussi une erreur. Le premier lecteur de smartcard était relié à une machine de vote qui était connectée pendant l'expérience pilote. Ce lecteur a été remplacé après avoir communiqué le problème à Smartmatic. Pour le second lecteur de smartcard, qui affichait des problèmes similaires, la machine de vote a été complètement remplacée. 4. Enfin, il y a eu aussi un problème avec l'imprimante d'une des machines de vote. Le petit couteau, avec lequel les bulletins de vote sont coupés, s'est calé et a bloqué la sortie de l'imprimante, ce qui a provoqué un bourrage de papier. Ce dernier a aussi été détecté par le test de diagnostic, mais pas pendant l'exécution des votes eux-mêmes. La machine de vote a été remplacée par Smartmatic. 		
Renvoi vers du matériel probant	OBR-009_Evidence.pdf		
Analyse d'impact			
Analyse d'impact :	La survenance limitée de tels problèmes pendant l'organisation des élections n'aura pas de grand impact. Mais si ce problème devait se présenter fréquemment, cela pourrait conduire à des retards significatifs dans le déroulement des élections.		
Recommandation			
Solution proposée :	Ces problèmes peuvent être résolus en testant suffisamment tous les hardwares. Ceci doit permettre de réduire considérablement les chances que de tels problèmes surviennent. On peut ainsi prévenir de graves problèmes.		
Résultat final			
Résultat final :	<p>A côté du duplicateur Kanguru, Smartmatic a fourni également un autre modèle de duplicateur, à savoir un AccuTower. Il a été également fourni une procédure pour l'utilisation des deux duplicateurs, où le risque de problèmes lors de la duplication est quasi nul et où la rapidité globale de duplication a significativement augmenté.</p> <p>Le problème avec l'un des lecteurs de smartcard pour un des appareils aurait dû être connu (modification incorrectement effectuée pour éviter l'électricité statique) et l'appareil en question aurait dû en fait être mis hors service au lieu d'être livré à PwC. De tels problèmes ne se présentent pas si la modification susmentionnée est réalisée de manière industrielle. Le problème avec l'autre lecteur de smartcard est une panne courante et continuera à être examiné.</p> <p>Le problème avec l'imprimante de la machine de vote sera examiné avec le fabricant des imprimantes.</p>		
Risque subsistant			
Estimation du risque subsistant après la réponse / la solution de Steria-Smartmatic			

Veuillez insérer la carte dans le bon sens
Voer de kaart correct in

Carte insérée dans le mauvais sens
Kaart werd niet correct ingevoerd

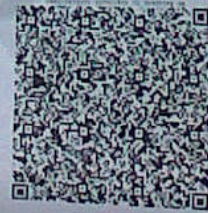
CLASSIFICATION: SECRET
CONTROLLED INFORMATION
EXCLUDED FROM AUTOMATIC
DOWNGRADING AND
DECLASSIFICATION



CLASSIFICATION: SECRET
CONTROLLED INFORMATION
EXCLUDED FROM AUTOMATIC
DOWNGRADING AND
DECLASSIFICATION



CLASSIFICATION: SECRET
CONTROLLED INFORMATION
EXCLUDED FROM AUTOMATIC
DOWNGRADING AND
DECLASSIFICATION





Genereren master geheugendrager

Genereren rapporten

Ontslutelen bestanden



Genereren rapporten

Via deze functionaliteit kunnen gebruikers rapporten voor de verkiezingen genereren

Rapport stembureau

Genereren rapporten

Stemlocatie	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
EVERGEM-001	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
EVERGEM-002	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
EVERGEM-003	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Vernieuwen

Alles selecteren

Fout



[REP-0000] - Er is geen printer geconfigureerd

Ok

< - Terug

Volgende ->



Rapport d'observation		Référence :	ROD-010
		Statut :	
Constat d'observation :	L'usage de la carte e-ID pour signer les procès-verbaux au niveau de la totalisation n'est pas conforme à la politique des cartes e-ID.		
Description			
Observé par :	Gaël Hachez	Date de l'observation :	19 December 2011
Contact :	gael.hachez@pwc.be		
Niveau d'importance :	B - demande une réponse/solution avant la fin de l'évaluation		
Module :	TOT Totalisation		
Activité au cours de laquelle l'observation a été faite :	La clôture de la totalisation et l'examen des procès-verbaux signés et des fichiers de résultats.		
Description détaillée de l'observation :	<p>Le cadre actuel qui est utilisé pour signer les procès-verbaux de manière électronique, ne permet pas de signature au moyen d'une carte e-ID. Le code PIN doit en effet être introduit pour chaque signature, ce qui n'est pas convivial. Pour contourner ce problème, une paire de clés locale est générée et la clé publique est certifiée au moyen de la carte e-ID. Techniquement, cette solution est suffisamment sécurisée si :</p> <p>(1) la clé privée n'est pas stockée sur un médium fixe ; et</p> <p>(2) il n'y a pas moyen de quitter le programme sans le redémarrer.</p> <p>En outre nous constatons que la signature consiste en une signature RSA avec un MD5 comme algorithme hash.</p>		
Renvoi vers du matériel probant	OBR-010_Signature.pdf		
Analyse d'impact			
Analyse d'impact :	<p>La mise en oeuvre actuelle de la signature électronique comporte deux problèmes :</p> <p>(1) Bien que cette solution soit techniquement possible, la certification d'une autre clé n'est pas une opération autorisée concernant l'usage des clés chargées sur la carte e-ID (EID certificate policy). A cause de cette limite, la signature pourrait ne pas être reconnue comme valable.</p> <p>(2) Pour le moment, seul le certificat local est chargé dans le fichier PDF. Il est donc impossible de vérifier la chaîne 'trust' via le certificat de la carte e-ID jusqu'au certificat 'root'. Par conséquent, la signature ne peut pas être validée.</p> <p>L'algorithme hash MD5 n'est plus résistant et ne peut donc pas être utilisé dans ce contexte.</p>		
Recommandation			
Solution proposée :	<p>Il y a deux solutions possibles :</p> <p>(1) Modifier le cadre de la signature. Il s'agit en effet ici d'une limite du cadre et pas de la carte e-ID. Des cadres alternatifs permettent bien la signature. Mais il faut préciser que ces cadres enfreignent une stricte interprétation de la loi : il faut donc rechercher du côté de l'Etat belge les motifs qui ont justifié l'introduction de cette limitation dans le cadre.</p> <p>(2) S'assurer que l'ensemble de la chaîne des certificats se retrouve dans le fichier PDF signé.</p> <p>Nous avons une préférence pour la solution (1) parce que celle-ci est plus transparente et qu'elle permet plus facilement de vérifier la signature de la personne en question, étant donné que c'est son nom qui apparaîtra en premier.</p> <p>L'algorithme MDS doit également être remplacé par un algorithme plus sécurisé, tel que SHA256.</p>		
Résultat final			
Résultat final :	Etant donné qu'il a été décidé au cours de la réunion du groupe de travail du 19/12/2011 que la signature des procès-verbaux interviendrait au niveau de l'application CODI, ce point tombe. Nous conseillons cependant que le fichier avec les résultats détaillés (X7S) soit malgré tout signé au moyen de la carte e-ID afin de garantir l'intégrité du fichier.		
Risque subsistant			
Estimation du risque subsistant après la réponse / la solution de Steria-Smartmatic	Il ne subsiste pas de risque si le fichier de résultats (X7S) sera directement signé avec la carte e-ID.		

At least one signature has problems.

Signatures

Validate All

Rev. 1: Signed by KANTON ZAVENTEM

Signature validity is unknown:

- Document has not been modified since this signature was applied
- Signer's identity is invalid because it has expired or is not yet valid
- Signing time is from the clock on the signer's computer.

Signature Details

Reason: CODI FILE PDF SIGNATURE
 Location: BELGIUM
 Certificate Details...
 Last Checked: 2011.12.20 11:58:39 +01'00'

Field: Signature1 on page 1
[Click to view this version](#)

STEMCIJFER(1) :

3



