Systèmes de vote électronique avec preuve papier

Avis

Smartmatic

Smartmatic

Avis 2018

Le 23 août 2018

Table des matières

NOTE IMPORTANTE

Ce document est une traduction de la version néerlandaise d.d. 23 août 2018. Ce document peut être utilisé à titre informatif, la version en néerlandaise étant la version valable en cas de discordances.

Un résumé de l'avis – Communauté germanophone et autorités wallonnes

Ministerin für lokale Behörden
Frau Isabelle Weykmans
Klötzerbahn 32
4700 Eupen

À l'attention de la Ministre des Pouvoirs locaux
Madame Valérie De Bue
Rue des Brigades d'Irlande 4
5100 Namur

Le 23 août 2018

Mesdames les Ministres,

Conformément à la convention conclue entre PwC et Smartmatic en date du 30 avril 2018 et en notre qualité d'organe consultatif pour les systèmes de vote numérique tels que décrits à l'article 11, §2, alinéa 2 de l'accord de coopération conclu le 13 juillet 2017 entre la Région wallonne et la Communauté germanophone concernant l'organisation des élections locales du 14 octobre 2018 sur le territoire de la région de langue allemande, nous avons réalisé un examen de la/des application(s) de vote électronique fournie(s) par Smartmatic, qui sera/seront implémentée(s) dans le cadre des élections du 14 octobre 2018 (ci-après dénommée(s), « l'Application »).

L'Application englobe plus spécifiquement :

- l'application liée à la conception d'un support permettant de créer des bureaux de vote ;
- le logiciel et le matériel informatique destinés au système du président ;
- le système de vote permettant à l'électeur d'exprimer et de contrôler son vote ;
- l'application d'enregistrement (urne) permettant de sauvegarder tous les votes électroniques exprimés.

Cet examen a pour but d'émettre un avis sur le caractère adéquat de l'Application.

Ce caractère adéquat porte sur les critères suivants :

- intégrité du processus électoral, résistance à la fraude, garantie de conservation du secret du scrutin ;
- conformité à la législation ;
- établissement d'un système fonctionnel, fiable, utilisable, efficace et pouvant être entretenu ; et
- établissement d'un système qui produit un résultat récurrent.

La conformité à la législation implique quant à elle la conformité aux dispositions suivantes :

- 22. April 2004: Kodex der lokalen Demokratie und der Dezentralisierung (für die Deutschsprachige Gemeinschaft anwendbare Fassung);
- Gemeindedekret vom 23. April 2018;
- Zusammenarbeitsabkommen (vom 13. Juli 2017) zwischen der Wallonischen Region und der Deutschsprachigen Gemeinschaft über die Lokalwahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
  Accord de coopération conclu le 13 juillet 2017 entre la Région wallonne et la Communauté germanophone concernant l'organisation des élections locales du 14 octobre 2018 sur le territoire de la région de langue allemande ;
- Dekret vom 23. Oktober 2017: Dekret zur Billigung des Zusammenarbeitsabkommens zwischen der Wallonischen Region und der Deutschsprachigen Gemeinschaft über die Lokalwahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
  Décret du 12 octobre 2017 : Décret portant assentiment à l'accord de coopération conclu le 13 juillet 2017 entre la Région wallonne et la Communauté germanophone concernant l'organisation des élections locales du 14 octobre 2018 sur le territoire de la région de langue allemande ;
- Zusammenarbeitsabkommen zwischen der Wallonischen Regierung und der Regierung der Deutschsprachigen Gemeinschaft zur Ausführung des Zusammenarbeitsabkommens vom 13. Juli 2017 zwischen der Wallonischen Region und der Deutschsprachigen Gemeinschaft über die Lokalwahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
- Erlass der Regierung vom 24. Mai 2018: Erlass der Regierung über die digitale Codierung, die digitale Übertragung und die automatisierte Verarbeitung der Wahldaten im Hinblick auf die Gemeinde- und Provinzialratswahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
- L'arrêté du Gouvernement wallon du 22 avril 2004, confirmé par le décret du 27 mai 2004, porte codification de la législation relative aux pouvoirs locaux, sous l'intitulé « Code de la démocratie locale et de la décentralisation » ;
- Arrêté du Gouvernement wallon du 19 avril 2018 : Arrêté du Gouvernement wallon modifiant l'arrêté du Gouvernement wallon du 7 juillet 2006 relatif à l'encodage numérique, la transmission numérique, ainsi qu'au traitement automatisé des données électorales ; et
- Lois sur l'emploi des langues en matière administrative, coordonnées le 18 juillet 1966.

Notre examen et l'évaluation de l'Application sont basés sur :

- un contrôle du traitement automatisé et du contrôle au sein des applications ;
- des entretiens avec la direction et d'autres membres du personnel de Smartmatic chargés de veiller au respect de la conformité aux conditions d'agrément ;
- le contrôle, sur la base de sondages, de documents qui démontrent le respect des conditions d'agrément ;
- la réalisation de tests de simulation, sur la base de sondages, sur un banc d'essai et une plate-forme d'essai ;
- le contrôle du code source, limité aux modifications résultant des demandes de modification introduites ; et
- les autres vérifications que nous jugeons nécessaires.

Nous avons plus spécifiquement évalué les étapes du processus et composants suivants :

- l'application de préparation, y compris le système de duplication ; et
- l'application utilisée au sein du bureau de vote :
  - le système du président ;
  - l'urne ; et
  - les machines à voter.
- L'application de recomptage.

Les observations reprises dans ce rapport ne portent que sur les versions finales de l'Application que Smartmatic a fournies à PwC le 15 mai 2018. Aussi bien dans l'application utilisée dans le bureau de vote (le

logiciel VOTE) que dans les fichiers de structure (lesdites « static data »), des problèmes entraînant un blocage ont encore été constatés dans le cadre du champ d'application de la présente évaluation.

C'est pourquoi les nouvelles applications suivantes ont été livrées :

- application de préparation, le 11 juillet 2018 (version 2.3.4-11072018133939) ; et
- application utilisée au sein du bureau de vote, le 11 juillet 2018 (version 2.2.12) et le 7 août 2018 (version 2.2.14).

Les modifications depuis la version du 15 mai 2018 ont été évaluées en réalisant des tests spécifiques afin d'évaluer les faiblesses résolues (OBR), complétés par un sous-ensemble du plan de test complet. Cependant, cela ne permet pas d'exclure le risque de régression[4].

Les modifications réalisées ou planifiées sur les applications et la documentation, postérieurement aux données précitées (p. ex., adaptations du logiciel pour remédier aux erreurs relevées) tombent explicitement en dehors du champ d'application de cette évaluation.

L'évaluation des conditions physiques (température, humidité, etc.) de stockage et d'utilisation des systèmes tombe en dehors du champ d'application de cette mission. Par ailleurs, l'exploitation opérationnelle des systèmes ne relève pas de la mission assignée à l'organe consultatif.

Parallèlement, nous notons que nos tests d'interface ne sont pas encore clôturés. Il s'agit des interfaces entre :

- les applications « gestion des candidats » (fichiers EML-230) et « gestion des contacts » (fichiers .csv) de CIVADIS, d'une part et l'application de préparation de Smartmatic, d'autre part ; et
- le système du président de Smartmatic et l'application « gestion des résultats » de CIVADIS (fichiers EML-510).

Sur la base des activités que nous exécutons dans le champ d'application de l'évaluation et pour autant que les instructions d'exploitation nécessaires soient mises en place et exécutées, et en référence à la définition du caractère adéquat mentionnée ci-dessus, nous arrivons à la conclusion, avec une certitude raisonnable[5] — mais non absolue — que l'Application est compatible avec le matériel informatique mis à disposition et répond aux critères du caractère adéquat définis ci-dessus.

L'extrapolation future de cette évaluation est sujette au risque de modification éventuelle des conditions d'agrément ou du degré de conformité de l'Application avec lesdites conditions.

La direction de Smartmatic est responsable de la conformité aux prescriptions législatives pertinentes, de l'adéquation et de la qualité des systèmes tels qu'ils ont été décrits ci-dessus.

Cet avis est uniquement établi à l'intention de la ministre des Pouvoirs locaux de la Communauté germanophone et de la ministre des Pouvoirs locaux des autorités wallonnes pour les élections locales du 14 octobre 2018.

Veuillez agréer nos salutations distinguées.

Floris Ampe[6]
Associé
PwC

[4] Par régression, nous entendons un problème éventuel qui pourrait apparaître lors de la résolution d'une erreur logicielle. L'erreur serait certes résolue par une modification, mais cette dernière pourrait alors occasionner d'autres erreurs.

[5] En ce qui concerne le terme « certitude raisonnable », nous nous référons à l'Arrêté royal du 26 mai 2002 relatif au système de Contrôle interne au sein des services publics fédéraux (MB 31 mai 2002).

[6] Floris Ampe scrl, administrateur délégué, représenté par son représentant permanent, Monsieur Koen Ampe.

Zusammenfassende Empfehlung – Deutschsprachige Gemeinschaft und Wallonische Regierung

Ministerin für lokale Behörden
Frau Isabelle Weykmans
Klötzerbahn 32
4700 Eupen

A l'attention de la Ministre des Pouvoirs locaux
Madame Valérie De Bue
Rue des Brigades d'Irlande 4
5100 Namur

23. August 2018

Sehr geehrte Minister,

gemäß der Vereinbarung zwischen PwC und Smartmatic vom 30. April 2018 und in der Eigenschaft als Beratungsgremium für digitale Wahlsysteme im Sinne von Artikel 11, §2, Absatz 2 des Zusammenarbeitsabkommens vom 13. Juli 2017 zwischen der Wallonischen Region und der Deutschsprachigen Gemeinschaft über die Lokalwahlen vom 14. Oktober 2018 im deutschen Sprachgebiet haben wir die von Smartmatic gelieferte(n) Anwendung(en) für elektronische Wahlen untersucht, die im Rahmen der Wahlen vom 14. Oktober 2018 verwendet wird/werden (nachstehend als die Anwendung bezeichnet).

Die Anwendung umfasst insbesondere:

- die Vorbereitungsanwendung, um ein Medium zu erstellen, um die Wahllokale zu starten;
- die Soft- und Hardware für das System des Vorsitzenden;
- das Wahlsystem für das Abgeben der Stimme durch einen Wähler sowie die Überprüfung seiner abgegebenen Stimme und
- die Registrierungsanwendung (Urne), um alle abgegebenen Stimmen elektronisch zu registrieren.

Ziel dieser Untersuchung ist es, eine Empfehlung über die Eignung der Anwendung abzugeben.

Diese Eignung umfasst:

- die Integrität des Wahlprozesses, Schutz gegen Betrug, Gewährleistung der Geheimhaltung der Abstimmung;
- die Einhaltung der Gesetzgebung;
- ein System, das funktionell, zuverlässig, brauchbar, effizient und wartbar ist und
- ein System, das zu einem wiederholbaren Ergebnis führt.

Die Einhaltung der Gesetzgebung umfasst ihrerseits die Einhaltung der folgenden Gesetzes- und Rechtsvorschriften:

- 22. April 2004: Kodex der lokalen Demokratie und der Dezentralisierung (für die Deutschsprachige Gemeinschaft anwendbare Fassung);
- Gemeindedekret vom 23. April 2018;
- Zusammenarbeitsabkommen (vom 13. Juli 2017) zwischen der Wallonischen Region und der Deutschsprachigen Gemeinschaft über die Lokalwahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
  Accord de coopération conclu le 13 juillet 2017 entre la Région wallonne et la Communauté germanophone concernant l'organisation des élections locales du 14 octobre 2018 sur le territoire de la région de langue allemande;
- Dekret vom 23. Oktober 2017: Dekret zur Billigung des Zusammenarbeitsabkommens zwischen der Wallonischen Region und der Deutschsprachigen Gemeinschaft über die Lokalwahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
  Décret de 12 octobre 2017: Décret portant assentiment à l'accord de coopération conclu le 13 juillet 2017 entre la Région wallonne et la Communauté germanophone concernant l'organisation des élections locales du 14 octobre 2018 sur le territoire de la région de langue allemande;
- Zusammenarbeitsabkommen zwischen der Wallonischen Regierung und der Regierung der Deutschsprachigen Gemeinschaft zur Ausführung des Zusammenarbeitsabkommens vom 13. Juli 2017 zwischen der Wallonischen Region und der Deutschsprachigen Gemeinschaft über die Lokal-wahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
- Erlass der Regierung vom 24. Mai 2018: Erlass der Regierung über die digitale Codierung, die digitale Übertragung und die automatisierte Verarbeitung der Wahldaten im Hinblick auf die Gemeinde- und Provinzialratswahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
- L'arrêté du Gouvernement wallon du 22 avril 2004, confirmé par le décret du 27 mai 2004, porte codification de la législation relative aux pouvoirs locaux, sous l'intitulé "Code de la démocratie locale et de la décentralisation";
- Arrêté du Gouvernement wallon de 19 avril 2018: AGW modifiant l'arrêté du Gouvernement wallon du 7 juillet 2006 relatif à l'encodage numérique, la transmission numérique, ainsi qu'au traitement automatisé des données électorales; en
- Die Gesetze über den Sprachengebrauch in Verwaltungsangelegenheiten, koordiniert am 18. Juli 1966.

Unsere Untersuchung und die Bewertung der Anwendung basieren auf:

- einer Überprüfung der automatisierten Verarbeitung und Kontrolle innerhalb der Anwendungen;
- Interviews mit dem Management und anderem Personal von Smartmatic mit zugewiesenen Aufgaben für die Einhaltung der Anerkennungsbedingungen;
- der stichprobenweisen Überprüfung von Dokumenten, die die Einhaltung der Anerkennungsbedingungen belegen;
- der Durchführung von Simulationstests auf Basis von Stichproben, mit einer Testbank und einer Testplattform;
- der Überprüfung des Quellcodes, beschränkt auf die Änderungen aufgrund der durchgeführten Änderungsanträge und
- sonstigen Überprüfungen, die wir als erforderlich betrachten.

Insbesondere haben wir die folgenden Verfahrensschritte und Komponenten bewertet:

- die Vorbereitungsanwendung, einschließlich des Duplizierungssystems und
- die innerhalb des Wahllokals verwendeten Anwendungen:
  - das System des Vorsitzenden,
  - die Urne,
  - die Abstimmungsgeräte und
- die Nachzählanwendung.

Die in diesen Bericht aufgenommenen Beobachtungen beziehen sich nur auf die letzten Versionen der Anwendung, die Smartmatic PwC am 15. Mai 2018 übergeben hat. In sowohl der Anwendung, die im Wahllokal verwendet wird (d. h. der VOTE-Software) als auch in den Strukturdateien (der sogenannten „static data“) wurden anfänglich innerhalb des Anwendungsbereichs der aktuellen Bewertung noch blockierende Probleme festgestellt.

Dafür wurden die folgenden neuen Anwendungen übergeben:

- am 11. Juli 2018 eine neue Version der Vorbereitungsanwendung (Version 2.3.4-11072018133939) und
- am 11. Juli 2018 (Version 2.2.12) und 7. August 2018 (Version 2.2.14) eine neue Version der im Wahllokal verwendeten Anwendung.

Die Änderungen seit der Version vom 15. Mai 2018 wurden durch die Durchführung spezieller Tests zur Bewertung der behobenen Schwächen (OBRs) bewertet, die um einen Teilsatz des vollständigen Testplans ergänzt wurden. Das Regressionsrisiko[7] ist damit jedoch nicht ausgeschlossen.

Andere Änderungen, die nach den oben genannten Terminen an den Anwendungen und der Dokumentation durchgeführt wurden oder geplant sind (d. h. Software-Anpassungen für die Behebung von Softwarefehlern) fallen ausdrücklich außerhalb des Anwendungsbereichs dieser Bewertung.

Die Bewertung der physischen Bedingungen (d. h. Temperatur, Feuchtigkeit usw.), unter denen die Systeme letztendlich gelagert und verwendet werden, fällt außerhalb des Anwendungsbereichs unseres Auftrags. Auch der operative Betrieb der Systeme fällt außerhalb des Auftrags des Beratungsgremiums.

Außerdem weisen wir darauf hin, dass unsere Schnittstellen-Tests gegenwärtig noch nicht abgeschlossen sind. Dies betrifft die Schnittstellen zwischen:

- den Kandidatenverwaltungs- (EML-230 Dateien) und Kontaktverwaltungs- (CSV-Dateien) Anwendungen von CIVADIS einerseits und der Vorbereitungsanwendung von Smartmatic andererseits und
- dem System des Vorsitzenden von Smartmatic und der Anwendung für die Ergebnisverwaltung von CIVADIS (EML-510 Dateien).

Auf Basis der von uns durchgeführten Arbeiten innerhalb des Anwendungsbereichs der Bewertung, unter der Bedingung, dass die erforderlichen Betreibungsanwendungen implementiert und durchgeführt werden und unter Hinweis auf die obige Definition der Eignung beschließen wir mit ziemlicher – jedoch keiner absoluten – Sicherheit,[8] dass die Anwendung mit der bereitgestellten Hardware kompatibel ist und die oben definierten Eignungskriterien erfüllt.

Die Extrapolation dieser Bewertung auf die Zukunft unterliegt dem Risiko, dass die Anerkennungsbedingungen oder das Maß der Konformität der Anwendung mit den Anerkennungsbedingungen geändert werden können.

Das Management von Smartmatic ist für die Einhaltung der einschlägigen Gesetzes- und Rechtsvorschriften, der Eignung und Qualität der Systeme, wie oben beschrieben, verantwortlich.

Diese Empfehlung ist nur für die Verwendung durch den Minister für lokale Behörden der Deutschsprachigen Gemeinschaft und den Minister für lokale Behörden der Wallonischen Regierung für die Lokalwahlen vom 14. Oktober 2018 bestimmt.

[7] Regression deutet auf das mögliche Problem hin, dass es bei der Lösung eines Softwarefehlers vorkommen kann, dass durch die Änderung zwar der Fehler gelöst wird, dies jedoch seinerseits andere Fehler verursachen kann.

[8] Für den Begriff „ziemliche Sicherheit“ verweisen wir auf den Königlichen Erlass vom 26. Mai 2002 über interne Kontrollsysteme innerhalb der Föderalbehörden (B. S. 31. Mai 2002).

Hochachtungsvoll,

Floris Ampe[9]
Teilhaber
PwC

[9] Floris Ampe bvba, Geschäftsführender Direktor, vertreten durch ihren ständigen Vertreter, Herrn Koen Ampe.

Introduction

Des élections locales seront organisées le 14 octobre 2018. Ce jour-là, le vote électronique sera possible dans un grand nombre de bureaux de vote. Le législateur prévoit que le Gouvernement compétent s'assure que les systèmes et processus numériques pour la gestion des candidats, le scrutin numérique, le traitement des votes et le calcul des sièges garantissent l'intégrité des données et le secret du scrutin. Pour pouvoir prendre une décision en connaissance de cause, le Gouvernement demande conseil à un organe consultatif agréé. L'organe consultatif contribue à la livraison d'applications fiables, de sorte que le citoyen puisse avoir la certitude qu'il pourra voter et que son vote sera correctement enregistré et traité.

En notre qualité d'organe consultatif, notre rôle consiste, dans le cadre de cette mission, à assister le Gouvernement compétent pour les parties de la solution « end-to-end » dont Smartmatic est responsable, à savoir l'application pour le vote électronique. Smartmatic fournit les systèmes pour la création des clés USB maîtres (à savoir l'application de préparation), les machines à voter, les urnes et les machines des présidents. Pour chacun de ces composants, Smartmatic fournit également les applications. Le déploiement des systèmes et leur exploitation le jour des élections ne font pas partie de l'objet de cette mission.

Depuis notre évaluation du système en 2014, dans le cadre des élections européennes, fédérales et régionales conjointes, différentes modifications ont été apportées au système ; le contexte (légal) dans lequel le système est utilisé a également évolué et l'utilisation du système de vote a été étendue. En Flandre, les habitants de 163 communes pourront dorénavant avoir recours au vote électronique. Dans la Région de Bruxelles-Capitale, l'utilisation du système de vote électronique sera étendue à 19 communes et au sein de la Communauté germanophone, le système de vote électronique Smartmatic sera utilisé pour les prochaines élections locales, en octobre.

À la suite de l'extension du système de vote électronique, Smartmatic va également introduire du nouveau matériel informatique (de nouvelle génération). Il a par ailleurs été décidé de lancer un projet pilote pour l'utilisation du module audio visant à soutenir les électeurs malvoyants. L'évaluation de la compatibilité du logiciel avec le matériel informatique de première génération et avec ce matériel informatique de nouvelle génération fait également partie de la mission de l'organe consultatif.

La mission dont résulte le rapport ci-dessous avait pour objectif d'évaluer l'adéquation du système de vote électronique avec preuve papier en vue de son utilisation pour l'organisation de toutes les élections et d'éventuelles élections combinées en Belgique. L'accent de la mission était toutefois porté sur l'évaluation des modifications apportées, d'une part, et l'évaluation du système dans le cadre de son utilisation lors des prochaines élections locales, en octobre.

Les chapitres suivants décrivent successivement l'objectif et le champ d'application de la mission, la méthodologie et l'approche que nous avons suivies et le résultat de notre évaluation technique.

Objectifs et délimitation de la mission

Objectifs

L'objectif final de la présente mission est de formuler un avis sur le caractère adéquat des systèmes proposés par Smartmatic.

Ce caractère adéquat porte sur les critères suivants :

- intégrité du processus électoral, résistance à la fraude, garantie de conservation du secret du scrutin ;
- conformité à la législation ;
- établissement d'un système fonctionnel, fiable, utilisable, efficace et pouvant être entretenu ; et
- établissement d'un système qui produit un résultat récurrent.

La conformité avec la législation se rapporte aux dispositions suivantes :

- Pour la Flandre :
  - Décret établissant l'organisation des élections locales et provinciales et amendant le décret communal du 15 juillet 2005, le décret provincial du 9 décembre 2005 et le décret du 19 décembre 2008 relatif à l'organisation des centres publics d'aide sociale [extrait cité : « Le décret électoral local et provincial du 8 juillet 2011 »] (coordination officieuse jusqu'au 01/06/2018) ;
  - Décret portant l'organisation du vote numérique lors des élections locales et provinciales [extrait cité : « le décret relatif à l'organisation d'élections numériques du 25 mai 2012 »] (coordination officieuse jusqu'au 01/06/2018) ;
  - Loi organique du 8 juillet 1976 relative aux centres publics d'action sociale (Communauté flamande) (coordination officieuse jusqu'au 15/02/2018) ;
  - Arrêté ministériel du 21 juin 2012 : Arrêté ministériel fixant les règles selon lesquelles les candidats figurant sur une liste de candidats sont visualisés sur l'écran d'un ordinateur de vote lors des élections locales et provinciales ;
  - Arrêté ministériel du 16 juillet 2012 : Arrêté ministériel fixant les caractères autorisés des noms de liste pour les élections locales et provinciales ; en
  - Arrêté ministériel du 31 mai 2018 : Arrêté ministériel modifiant l'annexe à l'arrêté ministériel du 13 juin 2012 fixant le système de vote numérique à utiliser lors des élections locales et provinciales et portant désignation des communes pouvant utiliser ce système de vote numérique.

- Pour la Région de Bruxelles-Capitale :
  - Code électoral pour la Région bruxelloise (coordination officieuse jusqu'au 01/06/2018) ;
  - Ordonnance organisant le vote électronique pour les élections communales (coordination officieuse jusqu'au 17/01/2018) ; et
  - Arrêté ministériel du 5 juin 2018 : Arrêté ministériel fixant les règles de présentation des listes et des candidats sur les écrans des machines à voter.

- Pour la Wallonie / la Communauté germanophone :
  - 22. April 2004: Kodex der lokalen Demokratie und der Dezentralisierung (für die Deutschsprachige Gemeinschaft anwendbare Fassung);
  - Gemeindedekret vom 23. April 2018;
  - Zusammenarbeitsabkommen (vom 13. Juli 2017) zwischen der Wallonischen Region und der Deutschsprachigen Gemeinschaft über die Lokalwahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
    Accord de coopération conclu le 13 juillet 2017 entre la Région wallonne et la Communauté germanophone concernant l'organisation des élections locales du 14 octobre 2018 sur le territoire de la région de langue allemande;

- Dekret vom 23. Oktober 2017: Dekret zur Billigung des Zusammenarbeitsabkommens zwischen der Wallonischen Region und der Deutschsprachigen Gemeinschaft über die Lokalwahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
  Décret du 12 octobre 2017 : Décret portant assentiment à l'accord de coopération conclu le 13 juillet 2017 entre la Région wallonne et la Communauté germanophone concernant l'organisation des élections locales du 14 octobre 2018 sur le territoire de la région de langue allemande ;
- Zusammenarbeitsabkommen zwischen der Wallonischen Regierung und der Regierung der Deutschsprachigen Gemeinschaft zur Ausführung des Zusammenarbeitsabkommens vom 13. Juli 2017 zwischen der Wallonischen Region und der Deutschsprachigen Gemeinschaft über die Lokalwahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
- Erlass der Regierung vom 24. Mai 2018: Erlass der Regierung über die digitale Codierung, die digitale Übertragung und die automatisierte Verarbeitung der Wahldaten im Hinblick auf die Gemeinde- und Provinzialratswahlen vom 14. Oktober 2018 auf dem deutschen Sprachgebiet;
- L'arrêté du Gouvernement wallon du 22 avril 2004, confirmé par le décret du 27 mai 2004, porte codification de la législation relative aux pouvoirs locaux, sous l'intitulé « Code de la démocratie locale et de la décentralisation » ; et
- Arrêté du Gouvernement wallon du 19 avril 2018 : Arrêté du Gouvernement wallon modifiant l'arrêté du Gouvernement wallon du 7 juillet 2006 relatif à l'encodage numérique, la transmission numérique, ainsi qu'au traitement automatisé des données électorales.

- Pour le SPF Intérieur
  - Code électoral (coordination officieuse jusqu'au 24/05/2018) et ses annexes ;
  - Loi du 23 mars 1989 relative à l'élection du Parlement européen (coordination officieuse jusqu'au 24/05/2018) ;
  - Loi ordinaire visant à achever la structure fédérale de l'État - L'élection du Parlement flamand et du Parlement wallon (coordination officieuse jusqu'au 24/05/2018) ;
  - Loi du 6 juillet 1990 réglant les modalités de l'élection du Parlement de la Communauté germanophone (coordination officieuse jusqu'au 24/05/2018) ;
  - Loi du 12 janvier 1989 réglant les modalités de l'élection du Parlement de la Région de Bruxelles-Capitale avec un extrait de la loi spéciale du 12 janvier 1989 relative aux institutions bruxelloises (coordination officieuse jusqu'au 24/05/2018) ; et
  - Loi du 7 février 2014 relative au vote électronique avec preuve papier (coordination officieuse jusqu'au 24/05/2018).

  Pour le SPF Intérieur, nous avons remarqué que dans les actuelles conditions d'agrément[17], il n'a pas encore été tenu compte du matériel nouvellement introduit (p.ex., le module audio, le clapet de l'urne électronique et l'utilisation d'un écran tactile pour le système du président).

- Généralités
  - Lois du 18 juillet 1966 sur l'emploi des langues en matière administrative.

[17] 21 mars 2014 - Arrêté royal fixant les conditions générales d'agrément des systèmes de vote électronique avec preuve papier - http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2014032105&table_name=loi

Champ d'application de la mission

Le champ d'application de notre mission est limité à une partie du processus électoral « end-to-end ». L'ensemble du processus électoral « end-to-end », avec indication du champ d'application de notre évaluation, est présenté dans le schéma ci-dessous.

Le champ d'application de notre mission se limite à l'application dans la partie « Vote », à savoir les étapes du processus et les composants suivants du logiciel :

- le système de préparation, y compris le système de duplication ;
- les systèmes utilisés au sein du bureau de vote :
  - le système du président ;
  - l'urne ; et
  - les machines à voter.
- l'application de recomptage.

Enfin, le champ d'application de notre mission comprend aussi, en ce qui concerne l'évaluation technique, la vérification de la compatibilité du logiciel avec le matériel informatique mis à disposition.

Le champ d'application de l'évaluation a été étendu, aux interfaces avec l'application MARTINE (fournie par CIVADIS) :

- des modules « Gestion des candidats » et « Gestion des contacts » au système de vote pour ce qui concerne les listes de candidats et les fichiers contenant les données du bureau de vote ; et
- du système de vote au module « Gestion des résultats » pour ce qui concerne les fichiers de résultats.

Les tests sont effectués de manière limitée et les tests « end-to-end » détaillés pour ces interfaces n'ont pas encore été entièrement clôturés. Pour le SPF Intérieur, ces tests « end-to-end » n'ont pas encore débuté et devront être réalisés avant que le système ne soit implémenté lors d'une élection (anticipée) ou lorsque les modules « Gestion des candidats », « Gestion des contacts » et « Gestion des résultats » de CIVADIS seront mis à disposition.

Éléments qui ne relèvent pas du champ d'application de cette évaluation

Le champ d'application de notre évaluation est limité aux éléments décrits ci-dessus comme faisant partie du champ d'application. Sont notamment explicitement exclus les éléments suivants :

- les applications de la partie « Gestion des candidats » (à savoir les applications « titulaire des listes électorales » (MA1L), « candidat » (MA1C), « signature des listes » (MA1S) et « bureau principal » (MA1B)) ;
- les applications de la partie « Gestion des résultats » (MA2x) ;
- l'application pour la partie « Gestion des contacts » (MA3x) ;
- les applications de la partie « Publication » ;
- le système de comptage numérique pour les bulletins de vote papier (DEPASS) ;
- l'exploitation des systèmes et l'exécution des procédures manuelles le jour des élections, y compris la configuration de l'application ;
- l'évaluation du matériel informatique et des infrastructures, tels que ceux qui seront utilisés dans le cadre de l'organisation des élections ; et
- l'appréciation des conditions physiques d'utilisation et de stockage des systèmes.

Base relative à l'évaluation technique

Les observations formulées dans le présent rapport se réfèrent uniquement aux versions testées par PwC à partir du 15 mai 2018, à savoir :

- Matériel informatique :
  - système de préparation, y compris le système de duplication (Accutower d'US Digital Media) ; et
  - système de vote : deux systèmes de président avec le matériel périphérique et les machines à voter, tous deux de la première comme de la deuxième génération.
- Logiciel :
  - logiciel ECM version 2.3.2-15052018145730 pour l'application de préparation ; et
  - logiciel VOTE version 2.2.4 pour l'application utilisée au sein du bureau de vote.

Aussi bien dans l'application utilisée dans le bureau de vote (le logiciel VOTE) que dans les fichiers de structure (lesdites « static data »), des observations avaient initialement été formulées dans le cadre du champ d'application de la présente évaluation, observations qui empêchaient d'arriver à un avis « adéquat » pour les élections. En outre, les autorités bruxelloises ont demandé de nouvelles modifications.

Ces observations ont été discutées en concertation par PwC et Smartmatic et un récapitulatif des observations entre-temps résolues figure dans le tableau de la rubrique « Risques ayant été corrigés grâce à des adaptations du logiciel » dans le chapitre « Résultat de l'évaluation technique ».

Afin de réévaluer ces observations et les modifications supplémentaires, PwC a reçu le 11 juillet 2018 une nouvelle version des différentes applications.

- logiciel ECM version 2.3.4-11072018133939 pour l'application de préparation ; et
- logiciel VOTE version 2.2.12 pour l'application utilisée au sein du bureau de vote.

Dans l'application utilisée dans le bureau de vote, de nouvelles observations ont été constatées dans le champ d'application de l'évaluation actuelle, qui empêchaient d'arriver à un avis « adéquat » pour les élections. Ces observations ont fait l'objet d'une concertation entre PwC et Smartmatic et sont reprises dans le récapitulatif des observations entre-temps résolues.

Afin de réévaluer ces observations, PwC a reçu le 7 août 2018 une nouvelle version du logiciel VOTE utilisé dans le bureau de vote, à savoir la version 2.2.14.

Le confort d'évaluation des modifications depuis la version du 15 mai 2018 a uniquement été obtenu en réalisant des tests spécifiques afin d'évaluer les faiblesses résolues (notamment les OBR de blocage), complétés par un sous-ensemble du plan de test. Cependant, cela ne permet pas d'exclure le risque de régression[18].

Le logiciel VOTE, version 2.2.14 doit être utilisé le jour des élections. Il faudra donc veiller à ce que la version du 7 août 2018 soit utilisée et non pas celles du 15 mai 2018 ou du 11 juillet 2018.

Pour plus de clarté, nous mentionnons ici les noms de fichiers et les codes de hachage de la version finale évaluée par nos soins, aussi bien pour le logiciel VOTE tel qu'il doit être utilisé lors de la génération de la clé USB maître, que pour le logiciel de génération des captures d'écran tel qu'il doit être utilisé lors de la création de la clé USB de génération des écrans :

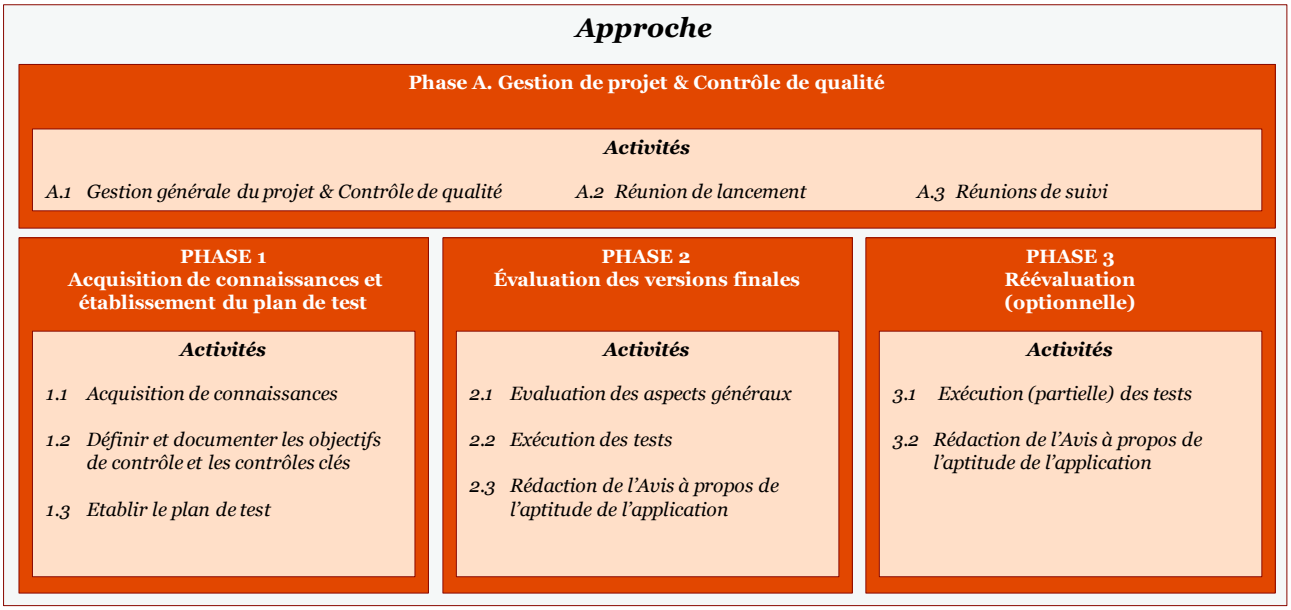
- logiciel VOTE :
  - OS-3.1.9_SW2.2.14_OFFICIAL_ECM.tar.gz
  - 4459714ccbe694605dac5feeec6d46d49a32ecf2971f0b8e2f7d90a477eb6c94
- génération des écrans :
  - OS-3.1.9_SW2.2.14_SCREEN_GENERATION_ECM.tar.gz
  - 9682f327dfbf4d760516e90a76bc6d2e2729fac9535767d21f0420ce9ee23d74

[18] Par régression, nous entendons un problème éventuel qui pourrait apparaître lors de la résolution d'une erreur logicielle. L'erreur serait certes résolue par une modification, mais cette dernière pourrait alors occasionner d'autres erreurs.

Méthodologie et approche

Aperçu général de l'approche

Le schéma ci-dessous donne un aperçu général de notre approche, qui précise les différentes activités lors de chacune des étapes.



Notre approche sera plus amplement détaillée dans ce chapitre. Les éléments suivants sont à chaque fois précisés pour chaque étape :

- Contenu de l'étape en question ; et
- Description des différentes activités de cette étape.

Approche par étape

Dans les sous-sections suivantes, les différentes étapes sont décrites plus en détail.

Étape 1 : Acquisition de connaissances et établissement du plan de test

Lors de cette étape, nous avons pris connaissance de la documentation (technique) et des systèmes mis à disposition par Smartmatic.

Ensuite, les objectifs de contrôle concrets ont été définis pour chaque partie spécifique du système. L'objectif de contrôle décrit le résultat souhaité ou l'objectif à atteindre par la mise en place de contrôles. Il s'agit des exigences minimales de contrôle effectif d'un processus ou d'un système spécifique. Nous avons ensuite également vérifié quels contrôles effectifs étaient nécessaires pour atteindre les objectifs de contrôle. Dans un premier temps, le processus des différents composants du système a été suivi et les contrôles prévus pour les différentes activités ont été définis et documentés.

Les principales sources utilisées pour définir les objectifs de contrôle et les contrôles sont énumérées ci-après :

- les exigences et les demandes de modifications approuvées ;
- la législation électorale ;
- le système lui-même ;
- la documentation des différents composants du système ; et
- notre expérience antérieure en tant qu'organe consultatif indépendant.

Lors de l'établissement du plan de test, nous avons également fait appel au Professeur Johan Ackaert (UHasselt). Ce dernier nous a assistés par ses connaissances en matière de législation électorale. Nous avons ainsi pu garantir que toutes les exigences légales, découlant directement de la législation électorale, ont aussi été reprises dans nos activités de contrôle.

Finalement, lors de cette étape, un plan de test détaillé a été établi, nous permettant de vérifier si les contrôles fonctionnaient également correctement. Dans le cadre de la vérification ou des tests de contrôles substantiels, nous avons réalisé quatre types de tests, à savoir :

- des tests fonctionnels ;
- des tests de scénarios et de volumes ;
- une analyse des fichiers de structure ;
- une analyse du code source ;
- une analyse des aspects de sécurité ;
- une évaluation de la documentation ; et
- une évaluation des interfaces.

Étape 2 : Évaluation des versions finales

Lors de cette étape, tous les tests prévus pour chacune des applications ont été réalisés étape par étape. Il s'agit des tests tels que décrits dans les plans de test ou activités de contrôle précités. Lors de l'exécution des tests, les documents probants ont à chaque fois été conservés, afin que nous puissions prouver que tous les tests nécessaires ont effectivement été réalisés. Une attention particulière a aussi été portée à la documentation des découvertes éventuelles (OBR). Cette étape débouche sur un rapport et sur notre Avis.

Étape 3 : Réévaluation

En cas de constatation de graves lacunes lors de l'évaluation, il est possible qu'après sa correction par Smartmatic, une réévaluation limitée d'une application spécifique ou de certaines parties doive être effectuée par l'organe consultatif.

Le pouvoir adjudicateur peut également demander des évaluations complémentaires après obtention de l'Avis. Ces évaluations complémentaires se limitent dans ce cas aux domaines qui ont été convenus avec le pouvoir adjudicateur.

En cas de réévaluation, l'approche sera globalement la même que celle de l'évaluation initiale. Il n'est cependant pas nécessaire de parcourir à nouveau la totalité du processus d'évaluation. Les objectifs de contrôle et les principaux contrôles mis en place pour le garantir sont en effet déjà connus. Dans la majorité des cas, il suffit d'exécuter à nouveau un sous-ensemble du plan de test existant ou d'obtenir d'une autre manière un confort d'évaluation suffisant, par exemple par quelques tests supplémentaires, spécifiquement ciblés sur la faiblesse résolue. Lorsque c'est possible, nous nous fions également au cadre de contrôle interne du pouvoir adjudicateur et aux tests effectués par le pouvoir adjudicateur afin d'obtenir un confort d'évaluation. Comme décrit précédemment, l'efficacité du cadre de contrôle interne du pouvoir adjudicateur est également évaluée.

Lors de cette étape également, un rapport d'observation est rédigé pour chaque observation supplémentaire éventuelle, ou les rapports d'observation issus des étapes précédentes feront l'objet d'un suivi ultérieur.

Résultat de l'évaluation technique

Ce chapitre dresse un aperçu, sur le plan du contenu, des observations effectuées. Pour de plus amples informations à ce sujet, notamment les rapports d'observation, nous vous renvoyons à l'Annexe A.

Nos observations (OBR) ont été classées en quatre catégories, l'utilisation d'un arbre décisionnel nous permettant de classer nos observations. Cet arbre décisionnel est présenté schématiquement dans ce chapitre.

Dans les sous-sections suivantes de ce chapitre, les observations sont reprises plus en détail selon les différentes catégories. Nous nous concentrons tout d'abord sur les observations liées au champ d'application de l'évaluation, qui n'ont pas encore été corrigées dans les versions testées par PwC et qui empêchent d'arriver à un avis « adéquat ».

Une deuxième sous-section comprend les observations liées au champ d'application de l'évaluation, qui n'ont pas encore été corrigées dans les versions testées par PwC, mais qui n'empêchent pas d'arriver à un avis « adéquat ».

Une troisième sous-section aborde les observations où les risques peuvent être corrigés grâce à des instructions d'exploitation (modifiées) ou une procédure manuelle.

La dernière sous-section comprend un aperçu des observations où les risques ont été corrigés grâce à une modification du logiciel.

Pour chaque observation, nous mentionnons pour quelle application et quelle élection elle est d'application.

À la fin de ce chapitre, nous aborderons un ensemble de points importants lors du déploiement et de l'exploitation des systèmes.

Le récapitulatif ci-dessous présente l'arbre décisionnel que nous avons utilisé pour classer nos observations.

Observations liées au champ d'application de l'évaluation, qui empêchent d'arriver à un avis « adéquat »

Lors de l'exécution de nos tests, nous n'avons identifié aucun risque dans les versions finales des systèmes qui n'ait pas encore été corrigé par Smartmatic.

Observations liées au champ d'application de l'évaluation, qui n'empêchent pas d'arriver à un avis « adéquat »

Lors de l'exécution de notre mission, nous avons, en lien avec le champ d'application de l'évaluation, constaté quelques problèmes pour lesquels il a été décidé qu'aucune correction ne devait être apportée. Cela est dû au fait que l'impact de ces problèmes est très limité et que les remarques ne donnent pas lieu à un avis « échec ». Nous conseillons uniquement d'améliorer ces points pour les élections lors desquelles ce système sera utilisé.

Vous trouverez ci-dessous un aperçu des observations qui ne constituent pas un blocage, mais qui sont susceptibles d'être améliorées lors d'élections. Pour de plus amples informations à ce sujet (à savoir les rapports d'observation), nous vous renvoyons à l'Annexe A.

Réf.	Observation	Module	Autorités / Élection
OBR-001	Le code source est documenté de manière limitée et contient des éléments qui ne sont pas applicables aux élections en Belgique.	Généralités	Toutes /Toutes
OBR-002	Les modifications cryptographiques RSA et SHA1 n'ont pas été remplacées de manière cohérente dans tout le code source.	Système du président et machines à voter	Toutes /Toutes
OBR-003	Un électeur peut opérer des sélections sur l'écran suivant avant que ce soit visible.	Machine à voter	Toutes /Toutes
OBR-004	Le titre du rapport des chiffres clés n'est pas parfaitement précis.	Système du président	SPF Intérieur / Toutes

Risques pouvant être corrigés grâce à des instructions d'exploitation (modifiées) ou une procédure manuelle lors d'une élection

Durant l'exécution de nos tests, nous avons constaté quelques problèmes pour lesquels il a été conclu qu'ils ne pouvaient ou ne devaient pas être corrigés par voie logicielle pour l'utilisation des systèmes lors des élections.

Ci-dessous, un aperçu des observations où les risques peuvent être corrigés grâce à des instructions d'exploitation (modifiées) ou une procédure manuelle. Pour de plus amples informations à ce sujet (à savoir les rapports d'observation), nous vous renvoyons à l'Annexe A.

Réf.	Observation	Module	Autorités / Élection
OBR-005	Le secret du vote peut être mis en péril lors d'un recomptage lorsqu'un seul électeur d'un type donné vote dans un bureau de vote donné.	Système du président et machines à voter	Toutes /Toutes
OBR-006	Les versions francophone et germanophone des instructions du module audio manquent de précision.	Machine à voter	Toutes /Toutes

Réf.	Observation	Module	Autorités / Élection
OBR-007	Sur la première génération de la machine à voter, le module audio peut être utilisé sans que des écouteurs soient branchés ; par conséquent le son est audible par tous.	Machine à voter	Toutes /Toutes

Les instructions d'exploitation (modifiées) ou les procédures manuelles en tant que contrôles alternatifs pour les risques qui ne peuvent pas être corrigés automatiquement, doivent être adoptées et suivies par les pouvoirs organisateurs. Le contrôle portant sur la rédaction et le respect de ces instructions et/ou procédures ne relève pas du champ d'application de notre mission.

Risques pouvant être corrigés grâce à des adaptations du logiciel

Lors de l'exécution de notre mission à partir du 15 mai 2018, nous avons constaté des problèmes qui empêchaient d'arriver à un avis « adéquat » et pour lesquels il a été décidé, en concertation avec Smartmatic, qu'il était nécessaire que ceux-ci soient corrigés pour le système proposé. Afin de réévaluer ces observations, PwC a reçu le 11 juillet 2018 et le 7 août 2018 de nouvelles versions des différentes applications.

Ci-dessous, un aperçu des observations où les risques ont été corrigés grâce à des modifications du logiciel.

Réf.	Observation	Module	Autorités / Élection
1	L'implémentation du droit de vote pour les élections directes des conseils du CPAS n'est pas conforme aux dispositions légales. Les citoyens non belges résidant à l'intérieur comme à l'extérieur de l'Union européenne ne peuvent pas voter aux élections directes des conseils du CPAS.	Système du président et machines à voter	VLA / CS
2	L'implémentation des différents types d'électeurs et de leur droit de vote n'est pas conforme aux dispositions légales.	Système du président et machines à voter	SPF Intérieur / Toutes
3	L'ordre dans lequel les différentes élections (les différents écrans) sont présentées aux électeurs n'est pas conforme aux dispositions légales.	Machine à voter	DG / CG + PR
4	La répartition des candidats en plusieurs colonnes n'est pas conforme aux dispositions légales.	Machine à voter	VLA+BRU+DG / Toutes
5	Les fichiers de structures contiennent des erreurs générant à leur tour des erreurs dans les applications.	Système du président et machines à voter	Toutes /Toutes
6	La répartition des listes et la possibilité de vote blanc ne sont pas conformes aux dispositions (légales).	Machine à voter	VLA+BRU+DG / Toutes

Légende :

Autorités	
SPF Intérieur	Autorités fédérales
VLA	Autorités flamandes
BRU	Région de Bruxelles-Capitale
DG	Communauté germanophone

Élections	
CS	Élection des conseils du CPAS
CG	Élections communales
PR	Élections provinciales

Points importants

Étant donné que cette évaluation est limitée au champ d'application décrit dans le chapitre « Champ d'application de l'évaluation pour ce rapport », le déploiement et l'exploitation des systèmes ne font pas partie de notre mission. Durant nos activités, nous avons toutefois relevé quelques points importants pour le bon fonctionnement des applications : Vous trouverez ci-dessous un aperçu non exhaustif de ces points importants.

- Les fichiers EML et .csv contenant respectivement les listes de candidats et les données des bureaux de vote doivent être signés avant de pouvoir être chargés dans les systèmes de préparation. Il est nécessaire que cette signature soit opérée à la source des données afin de pouvoir garantir l'intégrité des données entre la source (à savoir l'application pour la gestion des listes de candidats et les données des bureaux de vote) et l'utilisateur (à savoir le système de préparation).

- Nous souhaitons attirer l'attention sur l'importance de l'exécution d'un contrôle quant à l'exactitude et la complétude des fichiers contenant les données des bureaux de vote (les fichiers .csv) étant donné que ceux-ci contiennent des informations utilisées à plusieurs endroits de la chaîne. Ainsi, dans le système de préparation, par exemple, des mots de passe sont créés uniquement pour les bureaux de vote pour lesquels les données ont été chargées via un fichier .csv.

- Le pouvoir organisateur doit tenir compte du temps nécessaire pour accomplir toutes les tâches relatives au lancement et à l'utilisation du système de vote électronique. Nous recommandons par conséquent aux membres du bureau de vote de commencer à temps afin de garantir que toutes les tâches – y compris celles qui ne sont pas spécifiques au système de vote électronique (comme le fait de présenter serment par exemple) – puissent être réalisées avant l'ouverture du bureau de vote.

- En raison des différentes étapes de confirmation du processus de vote – a fortiori dans le cas d'élections simultanées –, il convient de tenir compte du temps plus important dont aura besoin un électeur pour pouvoir mener à bien le processus de vote. Nous souhaitons également souligner que le processus de vote avec l'utilisation du module audio nécessite un temps considérable.

- Les fichiers de résultats contenant les résultats du scrutin dans un bureau de vote spécifique sont cryptés par mesure de confidentialité. Ce cryptage s'effectue avec la clé publique d'une paire de clés pour laquelle l'application de consolidation et de répartition des sièges doit posséder la clé privée. De cette manière, l'application est en mesure de décrypter et de traiter les fichiers provenant des différents bureaux de vote. Naturellement, les parties impliquées auront préalablement convenu de la paire de clés utilisées, qu'elles auront échangées. Si les fichiers de résultats sont cryptés avec une clé incorrecte dans le bureau de vote, l'application de consolidation et de répartition des sièges ne sera pas en mesure de décrypter ni de traiter les résultats.

- Lorsque le rouleau de papier de la machine à voter est remplacé, il y a des chances que le code-barres du premier vote soit illisible. Cela est dû à la présence de colle sur le début du rouleau. Cela peut également endommager l'arrière de l'un des premiers billets imprimés par la suite (cela dépend de la longueur du billet imprimé), ce qui peut porter atteinte au secret du vote. Ces désagréments peuvent être évités en tirant suffisamment le papier à travers la fente lors du changement de rouleau afin que la partie endommagée soit coupée et éliminée par la machine à voter. Nous recommandons également d'utiliser un nouveau rouleau en début de journée.

- Étant donné l'utilisation de l'application de recomptage, il est possible que les clés USB des bureaux principaux de canton contiennent des résultats différents pour le même bureau de vote. Nous conseillons d'accorder une attention suffisante à la procédure de recomptage.

- La répartition de l'écran sur lequel les listes et la possibilité de vote blanc apparaissent suivent un algorithme précis (à savoir (Nombre de listes + vote blanc) / 4 = nombre de rangées (arrondi vers le haut)). Étant donné la façon dont cette fonctionnalité est mise en œuvre, cet algorithme est appliqué de la même façon pour toutes les élections et pour tous les pouvoirs organisateurs.
  En ce qui concerne la réglementation à ce sujet, seule la Région de Bruxelles-Capitale possède un arrêté ministériel (à savoir l'arrêté ministériel du 5 juin 2018 fixant les règles de présentation des listes et des

candidats sur les écrans des machines à voter). À l'Annexe 1 de cet arrêté ministériel, avec un aperçu de la répartition de l'écran présentant les listes sur la machine à voter, l'algorithme n'est toutefois pas respecté dans le cas où 24 options de choix sont proposées (c'est-à-dire 23 listes plus l'option de vote blanc). Selon le tableau d'aperçu, les 24 choix devraient être répartis en 4 colonnes de 7 lignes maximum. D'après l'algorithme, l'affichage doit comporter 6 lignes (23 + 1 / 4 = 6), ce qui a également été implémenté de cette façon dans le système.

- Au moment de l'évaluation, le manuel d'utilisation a été fourni en anglais uniquement. À cette époque, Smartmatic était encore en train de traduire ce manuel vers les différentes langues nationales requises.

- En ce qui concerne les élections organisées par les autorités fédérales, la nouvelle génération du matériel informatique n'est pas encore parfaitement conforme aux conditions générales d'agrément actuelles telles que définies dans l'arrêté royal du 21 mars 2014 fixant les conditions générales d'agrément des systèmes de vote électronique avec preuve papier. Dans cet AR, à l'article 2 par exemple, il est précisé que l'ordinateur du président est équipé d'un clavier. Pour la nouvelle génération, il s'agit d'un clavier tactile qui apparaît à l'écran lorsque c'est nécessaire. Il n'y a plus de clavier distinct. De plus, dans cet AR, il n'est fait aucune référence au clapet électronique fermant l'urne ni au module audio (si ce dernier devait être utilisé lors des élections organisées par les autorités fédérales).

- La situation décrite dans le document « Changements apportés au vote électronique avec preuve papier – propositions techniques et financières » relatif aux caractères autorisés dans le mot de passe du système du président ne correspond pas à l'implémentation. D'après le document, chiffres comme lettres peuvent être utilisés pour créer un mot de passe alors que dans la réalité, seules les lettres ont été implémentées. Actuellement, 23 caractères peuvent être utilisés pour générer un mot de passe pour le système du président. Dans le document, il est fait référence à 31 caractères possibles.

- Sur la base de notre examen du code source au départ d'une session de travail, nous constatons que la façon dont le système du président vérifie les mots de passe est vulnérable. Le mot de passe introduit est utilisé pour décrypter les fichiers de configuration. La manière dont les opérations de décryptage erronées sont traitées peut, dans certaines situations, mener au contournement du contrôle par mot de passe. Il est possible que ce contournement soit utilisé pour obtenir un accès non autorisé à certaines informations ou à certains composants du système.

- Nous avons constaté que la méthode de cryptage des fichiers de données conformément au mode opératoire CBC n'est pas à l'épreuve d'adaptations malveillantes. Les modifications apportées aux fichiers cryptés ne sont pas détectées par la fonctionnalité de décryptage dans le code source. Dans certaines situations, cela peut mener à un accès non autorisé à des informations sensibles.

La liste reprenant les points importants a uniquement été reprise à titre d'information et n'a pas pour objectif d'être exhaustive.

Annexes

Appendix A - Résultats détaillés de l'évaluation technique

Observations liées au champ d'application de l'évaluation, qui empêchent d'arriver à un avis « adéquat »

Aucune

Observations liées au champ d'application de l'évaluation, qui n'empêchent pas d'arriver à un avis « adéquat »

Réf.	Observation	Module	Autorités / Élection
OBR-001	Le code source est documenté de manière limitée et contient des éléments qui ne sont pas applicables aux élections en Belgique.	Généralités	Toutes /Toutes
OBR-002	Les modifications cryptographiques RSA et SHA1 n'ont pas été remplacées de manière cohérente dans tout le code source.	Système du président et machines à voter	Toutes /Toutes
OBR-003	Un électeur peut opérer des sélections sur l'écran suivant avant que ce soit visible.	Machine à voter	Toutes /Toutes
OBR-004	Le titre du rapport des chiffres clés n'est pas parfaitement précis.	Système du président	SPF Intérieur / Toutes

Risques pouvant être corrigés grâce à des instructions d'exploitation (modifiées) ou une procédure manuelle lors d'une élection

Réf.	Observation	Module	Autorités / Élection
OBR-005	Le secret du vote peut être mis en péril lors d'un recomptage lorsqu'un seul électeur d'un type donné vote dans un bureau de vote donné.	Système du président et machines à voter	Toutes /Toutes
OBR-006	Les versions francophone et germanophone des instructions du module audio manquent de précision.	Machine à voter	Toutes /Toutes
OBR-007	Sur la première génération de la machine à voter, le module audio peut être utilisé sans que des écouteurs soient branchés ; par conséquent le son est audible par tous.	Machine à voter	Toutes /Toutes

Rapport d'observation	Référence	OBR-001
Déclaration d'observation	Le code source est documenté de manière limitée et contient des éléments qui ne sont pas applicables aux élections en Belgique.	
Détails		
Module	Généralités	
Pouvoir organisateur / Élection	Tous / Toutes	
Activité pendant laquelle l'observation a été faite	Analyse du code source	
Description détaillée	La documentation du code source est insuffisante pour permettre son interprétation sans l'aide d'un programmeur. Nous souhaitons toutefois souligner que pour un non-programmeur, il est toujours difficile d'interpréter du code source. En outre, le niveau de détail de la documentation est une donnée subjective, qui est par nature discutable. Sur la base de notre analyse, nous pouvons constater que la documentation fournie devrait permettre à un programmeur de développer un concept au départ du code décrit. Nous avons remarqué que le code source contient encore des éléments qui ne sont pas applicables aux élections en Belgique. Quelques exemples de références aux textes espagnols relatifs au traitement des erreurs ont été relevés dans le fichier : « ECMApp_nl_BE.properties », « ECMApp_fr_BE.properties » et « ECMApp_de_BE.properties ». Les points ci-dessous donnent une liste non exhaustive : • CertificateUploadPanel.message.warning.upload=[CRT-0000] - Ocurrio un error al cargar los certificados. • ExceptionInfo.PROBLEM_GENERATING_DATABASE_BACKUP=[FGN-0030] â€“ Ocurrio un problema generando backup de la base de datos. • ExceptionInfo.PROBLEM_REACHING_DATA_BASE=[FGN-0031] â€“ No se puede alcanzar la base de datos para generar el backup. • WritingInPenDriveInfo.PEN_DRIVE_LABEL_DAMAGE=[USB-0010] - Ha ocurrido un error validando la etiqueta del pendrive o tiene una etiqueta invalida. Por favor asegÃºrese que el pendrive este formateado en formato EXT sin ninguna etiqueta.	
Preuve	Non applicable	
Analyse d'impact		
Analyse d'impact	La transparence et la maintenabilité du code source sont limitées. Nous souhaitons toutefois recommander la prudence lors de la suppression de tout code supposé superflu. Lors de la suppression de code, il est en effet toujours possible de supprimer accidentellement des éléments indispensables qui empêcheraient l'application de fonctionner correctement. De plus, il s'agit d'un processus fastidieux et long. Ce risque devra dès lors être évalué avec précision avant de prendre la décision d'« écrémer » le code.	
Solution		
Solution proposée	Nous proposons que le code source soit décrit de manière parfaitement transparente et de supprimer tous les éléments qui ne sont pas applicables aux élections en Belgique.	
Informations supplémentaires		

Risque subsistant	
Risque subsistant après réponse / solution	Le risque subsistant est limité étant donné qu'il n'a pas d'impact direct sur le fonctionnement ni sur les fonctionnalités du logiciel.
Classification finale	Observations liées au champ d'application de l'évaluation, qui n'empêchent pas d'arriver à un avis « adéquat »

Rapport d'observation	Référence	OBR-002
Déclaration d'observation	Les modifications cryptographiques RSA et SHA1 n'ont pas été remplacées de manière cohérente dans tout le code source.	
Détails		
Module	Système du président et machines à voter	
Pouvoir organisateur / Élection	Tous / Toutes	
Activité pendant laquelle l'observation a été faite	Examen du code source sur la base d'une session de travail Pour des explications et le champ d'application, voir remarque sous cet OBR.	
Description détaillée	<u>Système de préparation (ECM)</u> Dans le code source ECM actuellement utilisé (c'est-à-dire les « composants actifs du code source »), les fonctionnalités RSA et SHA1 ont été remplacées par les fonctionnalités ECC et SHA2. Dans le commentaire du code source et dans les composants qui ne sont pas utilisés activement (c'est-à-dire les « composants inactifs du code source »), les fonctionnalités RSA et SHA1 sont toujours présentes. <u>Système du président (PM)/système de vote (VM)</u> Les PM et VM sont implémentés sur la base de code source partagé. Dans ce code source, la fonctionnalité ECC a été ajoutée outre la fonctionnalité RSA existante. Par conséquent, les deux fonctionnalités sont prises en charge. La fonctionnalité qui sera exécutée dans le code source PM/VM est fonction des certificats fournis. À cet égard, Smartmatic suppose que la chance d'obtenir les certificats RSA est mince étant donné que les composants actifs du code source ECM ne prennent plus en charge que la fonctionnalité ECC. La fonctionnalité SHA1 dans le code source PM/VM relative aux signatures numériques et à l'authentification a été remplacée par la fonctionnalité SHA2. La fonctionnalité SHA1 est encore utilisée pour la transformation du mot de passe du président en clé cryptographique. Cette utilisation de la fonctionnalité SHA1 relève plus d'une dérivation de clé (« key derivation ») que d'une signature numérique et d'une authentification.	
Preuve	Constatation dans le code source durant les sessions de travail organisées	
Analyse d'impact		
Analyse d'impact	<u>Système de préparation (ECM)</u> La conservation des fonctionnalités RSA et SHA1 dans les composants inactifs du code source a un impact négatif sur la qualité du code source. En cas de modification du code source, cela peut entraîner une réactivation indésirable des fonctionnalités RSA et SHA1. <u>Système du président (PM)/système de vote (VM)</u> Faire dépendre la garantie de sécurité d'une application d'une supposition relative à l'obtention ou non d'un certificat n'est pas conforme aux directives de sécurité communément admises. Pour les systèmes PM/VM, cela signifie notamment en cas d'octroi des certificats RSA, que la fonctionnalité RSA sera encore exécutée dans l'application PM/VM.	
Solution		
Solution proposée	Remplacer toutes les références RSA et SHA1 dans les composants du code source, actifs comme inactifs, ainsi que dans les commentaires annexes.	

Informations supplémentaires	-
Risque subsistant	
Risque subsistant après réponse / solution	Actuellement, le risque subsistant est limité étant donné que nous avons constaté que cette adaptation avait été effectuée correctement. Le risque se situe toutefois au niveau des modifications futures, qui risqueraient de réactiver du code source erroné.
Classification finale	Observations liées au champ d'application de l'évaluation, qui n'empêchent pas d'arriver à un avis « adéquat »

Remarque :

Dans le cadre de l'étude du code source basée sur des sessions de travail, trois sessions de travail ont été organisées entre Smartmatic et PwC. Ces sessions de travail étaient systématiquement limitées dans le temps (4h) et organisées via vidéoconférence. Durant cette vidéoconférence, les parties pertinentes du code source Smartmatic ont été présentées par l'équipe de développement panaméenne de Smartmatic aux participants de PwC.

Ces sessions de travail virtuelles se sont déroulées conformément aux questions posées préalablement par PwC concernant les modifications pertinentes du code source. À la suite de la discussion avec l'équipe de développement, nous avons pu obtenir une meilleure vision de l'application et de la construction du code source. Les questions en découlant, qui étaient pertinentes pour les modifications de code source concernées, ont été posées durant les sessions de travail à l'équipe de développement.

L'approche adoptée à la suite de cette séance de travail est que PwC n'a pas examiné entièrement le code source lui-même. La bonne vision du code source obtenue et les modifications apportées au code source reposent entièrement sur les explications données par l'équipe de développement durant la vidéoconférence.

Rapport d'observation	Référence	OBR-003
Déclaration d'observation	Un électeur peut opérer des sélections sur l'écran suivant avant que ce soit visible.	
Détails		
Module	Machine à voter	
Pouvoir organisateur / Élection	Tous / Toutes	
Activité pendant laquelle l'observation a été faite	Tests du système de vote	
Description détaillée	Lorsqu'un électeur touche l'écran à une fréquence donnée, nous avons remarqué que les situations suivantes peuvent se produire : • Il est possible qu'un électeur fasse une sélection sur un écran qui n'a pas encore été chargé. Par exemple, après avoir touché le bouton de confirmation, l'électeur peut accidentellement toucher le bouton de retour à l'écran précédent. De même, cela peut se produire si, après avoir choisi un parti, l'électeur appuie rapidement ailleurs sur l'écran et, ce faisant, sélectionne déjà un candidat. Cependant, dans les deux cas, il faut que l'électeur touche deux fois rapidement l'écran à deux endroits différents. De plus, après avoir sélectionné la langue, une liste, ou un/des candidat(s), par exemple, l'électeur doit confirmer la sélection affichée. • Le bouton de confirmation n'apparaît qu'une fois une première sélection effectuée. L'affichage de ce bouton de confirmation après que l'électeur a fait un premier choix à l'écran peut entraîner une certaine confusion et faire penser à l'électeur qu'il doit déjà toucher le bouton « Confirmer » alors qu'il peut par exemple encore exprimer des votes nominatifs. • Lorsque l'électeur ne retire pas son doigt de l'écran et le fait glisser sur différents candidats, seuls quelques candidats sont sélectionnés. Cette sélection semble s'opérer de manière aléatoire.	
Preuve	Non applicable	
Analyse d'impact		
Analyse d'impact	L'électeur peut avoir l'impression qu'il ne dispose pas de la liberté de choix ou que le système est dans une « endless loop ».	
Solution		
Solution proposée	Nous proposons de résoudre par voie technologique le problème lors duquel une sélection est possible alors que l'écran n'a pas encore été chargé, afin de bloquer temporairement l'acceptation d'instructions complémentaires sur l'écran tactile du système de vote dès le moment où un choix a été opéré par l'électeur. Ce blocage doit avoir lieu jusqu'au moment où l'écran suivant est chargé et visible pour l'électeur. De cette manière, on évitera que le système de vote accepte des instructions pour des écrans qui ne sont pas encore visibles pour l'électeur au moment de la confirmation. Parallèlement, il est envisageable d'ajouter un écran de confirmation supplémentaire sur lequel seuls les choix effectués par l'électeur sont visibles. Sur cet écran supplémentaire, l'électeur devrait encore une fois confirmer son choix avant d'obtenir l'impression du ticket. Cette possibilité ralentit toutefois le processus de vote. Enfin, nous recommandons d'afficher les choix de menus dès le chargement de l'écran et non pas après qu'un candidat a été sélectionné.	

Informations supplémentaires	
Risque subsistant	
Risque subsistant après réponse / solution	Le nombre de manipulations indésirables est réduit.
Classification finale	Observations liées au champ d'application de l'évaluation, qui n'empêchent pas d'arriver à un avis « adéquat »

Rapport d'observation	Référence	OBR-004
Déclaration d'observation	Le titre du rapport des chiffres clés n'est pas parfaitement précis.	
Détails		
Module	Système du président	
Pouvoir organisateur / Élection	SPF Intérieur / Toutes	
Activité pendant laquelle l'observation a été faite	Tests du système de vote	
Description détaillée	Le titre du rapport des chiffres clés manque de précision dans le cas d'élections européennes, fédérales et régionales simultanées. En néerlandais, le titre est actuellement « Kerncijferrapport Federale verkiezingen (Europe/Kamer/Regionaal) - Vlaanderen ». En Région de Bruxelles-Capitale, dans le cas d'élections simultanées, le titre est actuellement « Kerncijferrapport Federale verkiezingen (Europees/kamer/regionaal) - BHG » / « Rapport des chiffres clés d'élections féderal (européenne/chambre/régional) - RBC ». Remarques : • Dans le rapport des chiffres clés en Flandre, nous avons relevé une faute de frappe : « Europe » ; • Dans la version néerlandaise, le titre n'est pas toujours le même alors qu'il s'agit de la même élection : « (Europe/Kamer/Regionaal) » en Flandre et « (Europees/kamer/regionaal) » pour la Région de Bruxelles-Capitale ; • En français, on peut lire « élections féderal » au lieu de « élections fédérales » ; • Il est fait référence à des « élections fédérales » alors qu'il s'agit en fait d'élections simultanées. Remarque supplémentaire : La date des élections simultanées du 26 mai 2019 est actuellement encore erronée dans le rapport des chiffres clés (25 mai 2019).	
Preuve	Non applicable	
Analyse d'impact		
Analyse d'impact	Des informations imprécises dans le titre du rapport des chiffres clés peuvent être trompeuses ou risquent de rendre le document non valable.	
Solution		
Solution proposée	Nous proposons que le document soit adapté de manière correcte et cohérente en concertation avec les pouvoirs organisateurs.	
Informations supplémentaires		
Risque subsistant		
Risque subsistant après réponse / solution	Moyennant l'adaptation correcte du document, le risque subsistant est relativement limité.	
Classification finale	Observations liées au champ d'application de l'évaluation, qui n'empêchent pas d'arriver à un avis « adéquat »	

Rapport d'observation	Référence	OBR-005
Déclaration d'observation	Le secret du vote peut être mis en péril lors d'un recomptage lorsqu'un seul électeur d'un type donné vote dans un bureau de vote donné.	
Détails		
Module	Système du président et machines à voter	
Pouvoir organisateur / Élection	Tous / Toutes	
Activité pendant laquelle l'observation a été faite	Test de la fonctionnalité de recomptage	
Description détaillée	Lors d'élections simultanées, éventuellement sous certaines conditions, des personnes ne possédant pas la nationalité belge ou des Belges habitant à l'étranger peuvent prendre part aux élections. Lorsqu'une seule personne appartenant à un type d'électeur donné vient voter et lorsqu'un recomptage est nécessaire, le secret du vote exprimé par cet électeur est mis en péril. En effet, en cas de recomptage, toutes les preuves papier doivent être rescannées avec l'urne électronique. La preuve papier de cette personne appartenant à un type d'électeur donné est cependant clairement reconnaissable étant donné qu'elle a participé à une ou plusieurs élections de moins que les électeurs belges.	
Preuve	Non applicable	
Analyse d'impact		
Analyse d'impact	Violation du secret du vote étant donné que les votes exprimés pour les différentes élections ne sont imprimés que sur une seule preuve papier commune et non pas sur des preuves distinctes pour chaque type d'élection.	
Solution		
Solution proposée	Nous proposons que le recomptage soit réalisé par des personnes qui n'ont pas été impliquées dans le processus de vote et qui ne connaissent par conséquent pas cet électeur unique venu voter. De cette manière, le secret du vote peut être garanti.	
Informations supplémentaires		
Risque subsistant		
Risque subsistant après réponse / solution	Moyennant l'introduction de procédures adéquates, le risque subsistant est relativement limité.	
Classification finale	Risques pouvant être corrigés grâce à des instructions d'exploitation (modifiées) ou une procédure manuelle lors d'une élection	

Rapport d'observation	Référence	OBR-006
Déclaration d'observation	Les versions francophone et germanophone des instructions du module audio manquent de précision.	
Détails		
Module	Machine à voter	
Pouvoir organisateur / Élection	Tous / Toutes	
Activité pendant laquelle l'observation a été faite	Tests du système de vote avec module audio	
Description détaillée	Nous avons remarqué que les versions francophone et germanophone des instructions du module audio (destiné aux électeurs malvoyants ou malentendants) manquaient de précision en cas d'utilisation du module audio de nouvelle génération sur la machine à voter. Nous avons relevé les erreurs suivantes : • Il est en effet fait référence à des boutons rectangulaires permettant d'adapter le volume alors que les boutons sur le module audio sont ronds. • Il est fait référence à un bouton carré au milieu alors que ce bouton est rond. • Il est fait référence à un petit bouton au bas du module permettant de répéter le dernier message prononcé alors qu'il y a deux boutons. Les instructions dans la version néerlandaise sont correctes. La formulation des instructions dans la version francophone n'est pas tout à fait correcte. Nous avons relevé les erreurs suivantes : • Il est fait référence à un « successeur candidat » alors que le terme communément utilisé est « suppléant ». • Le mot « secondes » est prononcé erronément « seconds ». • L'usage des temps dans la phrase n'est pas correct : « appuyez sur le bouton de confirmation rond lorsque vous entendiez l'option de votre préférence » devrait être « appuyez sur le bouton de confirmation rond lorsque vous entendez l'option de votre préférence ».	
Preuve	Non applicable	
Analyse d'impact		
Analyse d'impact	L'électeur qui utilise le module audio sur le matériel de nouvelle génération reçoit des instructions confuses ou erronées ne lui permettant pas d'achever le processus de vote de manière autonome.	
Solution		
Solution proposée	Nous proposons de vérifier la précision des instructions avant d'introduire l'utilisation du module audio lors des élections.	
Informations supplémentaires		
Risque subsistant		
Risque subsistant après réponse / solution	Moyennant l'introduction de procédures adéquates, le risque subsistant est relativement limité.	
Classification finale	Risques pouvant être corrigés grâce à des instructions d'exploitation (modifiées) ou une procédure manuelle lors d'une élection	

Rapport d'observation	Référence	OBR-007
Déclaration d'observation	Sur la première génération de la machine à voter, le module audio peut être utilisé sans que des écouteurs soient branchés ; par conséquent le son est audible par tous.	
Détails		
Module	Machine à voter	
Pouvoir organisateur / Élection	Tous / Toutes	
Activité pendant laquelle l'observation a été faite	Tests du système de vote avec module audio	
Description détaillée	Nous avons remarqué qu'il est possible, sur la première génération de machines à voter, d'utiliser le module audio (conçu pour les électeurs malvoyants ou malentendants) sans que des écouteurs ne soient branchés : • il est possible de débuter le processus de vote sans que des écouteurs ne soient branchés ; ou • les écouteurs peuvent également être déconnectés durant le vote. Dans les deux cas, le son est alors envoyé vers les haut-parleurs de la machine à voter et le volume est suffisamment élevé pour que toutes les autres personnes se trouvant à une certaine distance puissent entendre clairement.	
Preuve	Non applicable	
Analyse d'impact		
Analyse d'impact	Si le son du module audio est audible par de tierces personnes durant le vote, le secret du vote n'est plus garanti.	
Solution		
Solution proposée	Nous proposons de débrancher le haut-parleur des machines à voter de première génération afin que le son du module audio ne puisse être diffusé via cette voie.	
Informations supplémentaires		
Risque subsistant		
Risque subsistant après réponse / solution	Moyennant l'introduction de procédures adéquates, le risque subsistant est relativement limité.	
Classification finale	Risques pouvant être corrigés grâce à des instructions d'exploitation (modifiées) ou une procédure manuelle lors d'une élection	

Appendix B - Sommes de contrôle

PwC – Smartmatic – Official delivery – 07/08/2018

Hashes method: SHA256

ECM

Applications/ECM/app-client-2.3.4-11072018133939.zip
595b4b96028b1a56f0b909b58a556ba5d6c817b0877c3826022f1a0910dc83d9

Applications/ECM/app-jboss-2.3.4-11072018133939.zip
1a45da2e3108a3b854cde0ebe302cc94ce38990a2839701e4f37b33999600a2b

Applications/ECM/app-database-2.3.4-11072018133939.zip
f55f8c65cadfed3e6bcc0cf8a2d0cc1a88eceb5ac097f4e52a027bdd81f11eea

OS-Images/ECM/OS-UBUNTU-14.04.5-1.0.2-11072018133959-ECM-2.3.4-11072018133939.iso
51bc34e5c73ea3db75bf4d0dd74fe5e6c2746debcc4d99c3e8e28e209a8ed309

PM/VM

6ad76aabd86daf87077f92173c62880cc9c82d4f7d72b60a04b41c368678632a
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-printer-config_1.0.0_all.deb

4b2b5acf7317d9aec3404a5a8a6e50e8ce5e0ae332665458c9145c064047a7f9
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-os-xorg-config_1.0.0_all.deb

1c765312ffff4e206b18ca60ec757df59e8f92fa30c9beb2b2af58b653039b85
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-os-dsort-config_1.0.0_all.deb

94d45b3adc79388231e32d3c748b8f2d3d57f73355a442e44b1aaf838c204a22
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-os-splash-config_1.0.0_all.deb

f55d2c9accbcb2b65c7ac99265e0400446abd4f625f8dd4642a1a5d9e96de128
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-audio-config_1.0.0_all.deb

465cb0c09173e794d218ab2f02b04ed9fc28e295cbad1142ab13eeca6da6b133
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-os-usb-devices-config_1.0.0_all.deb

d2fbf2cc1114a689e3d1749e2510bf46b8140610d5fd8240d3a6c04570357325
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-os-scr-config_1.0.0_all.deb

ea0255fd5882c779e3d47719331b2947479590057948a822f39e6473fc5a02cd
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-os-load-election_1.0.0_all.deb

3287369c090e502e46406a2a85644bf27f82e766953fc060a5208fae125ef92c
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-os-info-machine_1.0.0_all.deb

6592685c0c2c5a2d81d517eaf33824206f2ec453d835d86d34975cd879f69bc3
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-serial-touch-calibration_1.0.0_all.deb

c87fa404db31d5f999401c30cc6aeceec85a35b51183141ba09869a6198bb51b
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-os-serial-config_1.0.0_all.deb

59e343685c6644254dd55b6ceea98e52071b4af6c39604740be9abc223d3a554
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-os-sealed-config_1.0.0_all.deb

90d9edeb0e7c51d050b0ee2ad166dcf3bfaa252c3aea8f1dfde538668adf43f2
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/os-config/smtt-os-xorg-config-a4500_1.0.0_all.deb

7e4463560b7bb01e5c129c33e24fbce834c6d8fc86742b6de41d9a6a1e585712
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/printer-driver-ib31k1-0.1.0-i386.deb

cede842776a986173dff88500ad1d191bc274b4a41859676d0a9a27a6f3c4034
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/gppcscconnectionplugin-lib_1.0.1-1_i386.deb

e7bda58c79c6ec71e44f17b37bef53554d7fb40acf5ca7b8f7232bec0fcbce62
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/nuance-vocalizer-dev_5.32-1_i386.deb

ffd80a466faf52fa8c25b9a927ffaf28797efdbf83f58bce976642ec5b928d8d
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/libxml-security-c17_1.7.3-smartmatic_i386.deb

c3e2d69ca0aec9972ce6218b9de32e6cbb32f69b69693d0f0bdffd7e2a83494d
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/penmount_1.0.0_i386.deb

21187a6ad1a50aaffc9b898b6d8f78813152153b4046a69c4b5ace70f9303d9a
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/aps_0.16.2_i386-dev.deb

000646d0722883f1dc116dd094a7ef78832da234b5612f3d77f94e6cabad7589
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/globalplatform-lib_6.0.0-1_i386.deb

68f6680c6db697945a4c14c5ab5fdda1560a9a20097dff11c281cbc5d43d6a1e
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/nuance-vocalizer-lib_5.32-1_i386.deb

31496978357da15a34073f08ddae4a0627ac0010013a4025e31c9cfadef53f95
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/aps_0.16.2_i386-lib.deb

2d22acf6353b706eb1d2976183bf70d1e6282633f8c51b105ee52c8effc5fe00
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/via_1.0.0_i386.deb

d7df01374dac66ef50bae09ae03624d0b8b86c937d60818e5dd3212abec4279c
OfficialDeliveryProcessOutput/CustomDEB/PM-VM/third-party/globalplatform-dev_6.0.0-1_i386.deb

caa5b2d7dd6368bea9259afdb840ee095a04e364f1c304e2c49e3825c4f6e56a
OfficialDeliveryProcessOutput/Applications/PM-VM/election-conf-technician-diagnostic_2.2.14-1_i386.deb

4f5b89460f475d8d8a96b79520726f5ff789a2f2a0ead3d83744ebba06cfceaf
OfficialDeliveryProcessOutput/Applications/PM-VM/election-conf-data-validator_2.2.14-1_i386.deb

08001e98b9ff912fc63334082f591b4533536f69a0fc9749d56173481bbf6d8b
OfficialDeliveryProcessOutput/Applications/PM-VM/election-conf-training_2.2.14-1_i386.deb

5edc447152ba994ad5ec88ffdf5e6837f062f350bd148b7db8f5302776a70b45
OfficialDeliveryProcessOutput/Applications/PM-VM/election-conf-demo_2.2.14-1_i386.deb

030aaa804c5a26969730e3770dbd62a584cc65500dcbf51767e0ef7327b28323
OfficialDeliveryProcessOutput/Applications/PM-VM/election-themes_2.2.14-1_i386.deb

e0760575f3358053ccff9e5d34e8a76ed27fd83882392c4b061dae303589f385
OfficialDeliveryProcessOutput/Applications/PM-VM/election-lib_2.2.14-1_i386.deb

812c46553032b1e0a018a782b304cd548938a1c913589585fd1bf857fba7a2c6
OfficialDeliveryProcessOutput/Applications/PM-VM/election-conf-communes-diagnostic_2.2.14-1_i386.deb

d39748baa9dc958f40b2483b033898e47dbf6e03a766f307c0cea3e3918eba38
OfficialDeliveryProcessOutput/Applications/PM-VM/election-conf-official_2.2.14-1_i386.deb

9863e8db137eaef477a02dc53a2cc48aaa1ad0506304576d4601f9850ba749e6
OfficialDeliveryProcessOutput/Applications/PM-VM/election-l10n_2.2.14-1_i386.deb

22325d41a9eb8092cbcbb885a7453f583d3b56f212961b8e6a92b34d0665c5e4
OfficialDeliveryProcessOutput/Applications/PM-VM/election-conf-screen-generator_2.2.14-1_i386.deb

0ba38db92bff440ab7647bf9b81096cd51e7513dc440a04eb321f54a5fb8d3ae
OfficialDeliveryProcessOutput/Applications/PM-VM/election-app_2.2.14-1_i386.deb

85055f6bdb8d0e7dd02d59f9d22e545d4aca7ee67ef2108ecdb9174caf2f952d
OfficialDeliveryProcessOutput/Applications/PM-VM/election-dev_2.2.14-1_i386.deb

PM/VM Training mode
357d4ab4f7a6a2b939a862c7ceb1eaed3027f664f109936aed0848628d018486
OfficialDeliveryProcessOutput/OS-Images/PM-VM/OS-3.1.9_SW2.2.14_TRAINING_ECM.tar.gz

PM/VM Demo mode
7cb997036f99b47da7c28e418244a785542353245dc332bb27ee7fac18f94946
OfficialDeliveryProcessOutput/OS-Images/PM-VM/OS-3.1.9_SW2.2.14_VOTER_DEMO_ECM.tar.gz

PM/VM Diagnostics
28fd9ca597202f11297862dceb0108f244ca9bd26d81fe305e1f6e352a771069
OfficialDeliveryProcessOutput/OS-Images/PM-VM/OS-3.1.9_SW2.2.14_DIAGNOSTIC_TECHNICIAN_NL.tar.gz

13af5e59c0cf47c123d55ae73dfd23ac6283be94660cde9b03c5dd66102f30ea
OfficialDeliveryProcessOutput/OS-Images/PM-VM/OS-3.1.9_SW2.2.14_DIAGNOSTIC_TECHNICIAN_FR.tar.gz

d93bc2cd363d16bd3ce722affc78934dffa98620887433938c958d36461df422
OfficialDeliveryProcessOutput/OS-Images/PM-VM/OS-3.1.9_SW2.2.14_DIAGNOSTIC_COMMUNES_FR.tar.gz

1018f5708c56568b881079c7f4367f0a65ede7d13e4827a187fb639ed70e3943
OfficialDeliveryProcessOutput/OS-Images/PM-VM/OS-3.1.9_SW2.2.14_DIAGNOSTIC_COMMUNES_DE.tar.gz

0171b311b47b88c57081e8609ff58642c3e747e4f3b94d5cbd8bbccce0260c78
OfficialDeliveryProcessOutput/OS-Images/PM-VM/OS-3.1.9_SW2.2.14_DIAGNOSTIC_TECHNICIAN_DE.tar.gz

37684900c717c37daf2f43a852086d2dd58217fbe4e96b1216cecca2d8c096e9
OfficialDeliveryProcessOutput/OS-Images/PM-VM/OS-3.1.9_SW2.2.14_DIAGNOSTIC_COMMUNES_NL.tar.gz

Compilation Cache PM/VM
00b97edfcb208ddd844d19f9c16d11227308e8063850712f1f45a4805a6e54c6
PM-VM-Cache/bevoting-cacher-20180807_1324.tar.gz

Hash to appear in the ECM during Master USB creation

PM/VM Software

4459714ccbe694605dac5feeec6d46d49a32ecf2971f0b8e2f7d90a477eb6c94
OfficialDeliveryProcessOutput/OS-Images/PM-VM/OS-3.1.9_SW2.2.14_OFFICIAL_ECM.tar.gz

Screen generator

9682f327dfbf4d760516e90a76bc6d2e2729fac9535767d21f0420ce9ee23d74
OfficialDeliveryProcessOutput/OS-Images/PM-VM/OS-3.1.9_SW2.2.14_SCREEN_GENERATION_ECM.tar.gz