SERVICE PUBLIC FEDERAL INTERIEUR

[C − 2019/40410]

4 MARS 2019. — Arrêté ministériel déterminant les conditions d'agrément des logiciels utilisés pour le recensement électronique des voix par les bureaux de dépouillement lors des élections du Parlement européen, de la Chambre des représentants, du Parlement wallon, du Parlement flamand, du Parlement de la Région de Bruxelles-Capitale, des membres bruxellois du Parlement flamand et du Parlement de la Communauté germanophone

Le Ministre de la Sécurité et de l'Intérieur,

Vu le Code électoral, article 165, alinéa 4, modifié par la loi du 19 avril 2018;

Vu les lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973, notamment l'article 3, § 1er, alinéa 1er;

Vu l'urgence;

Considérant que le dépôt des candidatures pour les élections simultanées du 26 mai 2019 du Parlement européen, de la Chambre des représentants, du Parlement wallon, du Parlement flamand, du Parlement de la Région de Bruxelles-Capitale, des membres bruxellois du Parlement flamand et du Parlement de la Communauté germanophone est fixé au vendredi 29 mars 2019 et au samedi 30 mars 2019; qu'il est dès lors impératif de déterminer sans tarder les conditions d'agrément des logiciels utilisés pour le recensement électronique des voix par les bureaux de dépouillement lors de ces élections,

Arrête :

Article 1er. Les logiciels visés à l'article 165, alinéa 4, du Code électoral, qui sont utilisés pour le recensement électronique des voix par les bureaux de dépouillement peuvent recevoir un avis positif d'un organisme, reconnu à cette fin par le Roi par arrêté délibéré en Conseil des Ministres, si ils satisfont aux conditions émises à l'article 2 du présent arrêté.

Art. 2. Le système assure le dépouillement des bulletins de vote provenant des bureaux de vote papier.

A. Généralités

Plusieurs élections sont possibles:

- Organisées par l'Etat fédéral:

* Élections européennes;

* Élections fédérales;

* Élections régionales pour:

> le Parlement flamand;

> le Parlement wallon;

> le Parlement de la Région de Bruxelles-Capitale;

> le Parlement de la Communauté germanophone.

Le système doit supporter toutes ces élections ainsi que toutes les combinaisons possibles de 2 ou plusieurs élections relevant simultanément d'une même autorité organisatrice et ce, par le biais de la configuration des paramètres, par exemple des élections européennes, fédérales et régionales ou des élections fédérales et des élections régionales pour le Parlement flamand, pour l'Etat fédéral.

Un seul type d'élection sera dépouillé par bureau de dépouillement.

Informations de contexte, la procédure actuelle pour le dépouillement manuel pour les élections organisées par l'Etat fédéral: Chaque bureau de dépouillement collecte les bulletins de vote papier d'un ou de plusieurs bureaux de vote (normalement 3 bureaux de vote = maximum 2400 bulletins de vote). Ils sont mélangés, mis en tas et comptés. Ils sont ensuite répartis en trois tas: les bulletins de vote valables; les bulletins de vote nuls ou blancs; les bulletins de vote imprécis.

Tout bulletin de vote imprécis est examiné et évalué par l'ensemble du bureau de dépouillement (éventuellement au moyen d'un vote) et sont alors ajoutés au tas des bulletins de vote valables ou au tas des bulletins de vote nuls et blancs. Il ne reste ainsi que 2 tas. Les bulletins de vote nuls ou blancs sont comptés. Le nombre est noté sur le formulaire prévu.

Les bulletins de vote valables sont répartis en 4 sous-catégories (SC) par parti: les bulletins avec uniquement des votes en tête de liste (SC1); les bulletins de vote uniquement en faveur de candidat(s) titulaire(s) (SC2); les bulletins de vote en faveur de candidat(s) titulaire(s) et de candidat(s) suppléant(s) (si d'application) (SC3); les bulletins de vote en faveur uniquement de candidat(s) suppléant(s) (SC4).

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN

[C − 2019/40410]

4 MAART 2019. — Ministerieel besluit tot vastlegging van de erkenningsvoorwaarden voor de software die door de stemopnemingsbureaus voor de elektronische stemmentelling gebruikt wordt bij de verkiezingen van het Europees Parlement, de Kamer van Volksvertegenwoordigers, het Vlaams Parlement, het Waals Parlement, het Parlement van het Brussels Hoofdstedelijk Gewest, de Brusselse leden van het Vlaams Parlement en het Parlement van de Duitstalige Gemeenschap

De Minister van Veiligheid en Binnenlandse Zaken,

Gelet op artikel 165, vierde lid, van het Kieswetboek, gewijzigd door de wet van 19 april 2018;

Gelet op de wetten op de Raad van State, gecoördineerd op 12 januari 1973, inzonderheid op artikel 3, § 1, eerste lid;

Gelet op de dringendheid;

Overwegende dat de indiening van de kandidaturen voor de gelijktijdige verkiezingen van 26 mei 2019 van het Europees Parlement, de Kamer van Volksvertegenwoordigers, het Vlaams Parlement, het Waals Parlement, het Parlement van het Brussels Hoofdstedelijk Gewest, de Brusselse leden van het Vlaams Parlement en het Parlement van de Duitstalige Gemeenschap vastgelegd werd op vrijdag 29 maart 2019 en zaterdag 30 maart 2019; dat derhalve onmiddellijk de erkenningsvoorwaarden bepaald moeten worden voor de software die door de stemopnemingsbureaus voor de elektronische stemmentelling gebruikt wordt bij die verkiezingen,

Besluit :

Artikel 1. De in artikel 165, vierde lid, van het Kieswetboek bedoelde software die door de stemopnemingsbureaus gebruikt wordt voor de elektronische stemmentelling, mag een positief advies krijgen van een instantie, daartoe door de Koning erkend bij een in Ministerraad overlegd besluit, als ze voldoet aan de voorwaarden opgesomd in artikel 2 van dit besluit.

Art. 2. Het systeem zorgt voor het tellen van de stembiljetten afkomstig van de papieren stembureaus.

A. Algemeen

Er zijn verschillende verkiezingen mogelijk:

- Georganiseerd door de federale overheid:

* Europese verkiezingen;

* Federale verkiezingen;

* Regionale verkiezingen voor:

> het Vlaams Parlement;

> het Waals parlement;

> het Brussels Hoofdstedelijk Parlement;

> het Parlement van de Duitstalige Gemeenschap;

Het systeem moet al deze verkiezingen ondersteunen evenals alle mogelijke combinaties van 2 of meerdere verkiezingen tegelijk behorend tot een zelfde organiserende overheid via het configureren van parameters, bijvoorbeeld Europese, federale en regionale verkiezingen of federale verkiezingen en regionale verkiezingen voor het Vlaams Parlement voor de federale overheid.

Per telbureau zal er slechts één soort verkiezing worden geteld.

Achtergrondinformatie, de huidige procedure voor het manueel tellen voor de verkiezingen georganiseerd door de federale overheid: Per telbureau worden de papieren stembiljetten van één of meerdere stembureaus verzameld (normaal 3 stembureaus = maximaal 2400 stembiljetten). Hier worden ze gemengd, op een stapel gelegd en geteld. Daarna worden er 3 stapels gemaakt: de geldige stembiljetten; de ongeldige of blanco stembiljetten; de onduidelijke stembiljetten.

Elk onduidelijk stembiljet wordt door het volledige telbureau bekeken en beoordeeld (eventueel d.m.v. stemming) en worden dan toegevoegd aan de stapel met de geldige stembiljetten of de stapel met de ongeldige en blanco stembiljetten. Zo blijven er nog slechts 2 stapels over. De ongeldige of blanco stembiljetten worden geteld. Het aantal wordt genoteerd op het voorziene formulier.

De geldige stembiljetten worden per partij onderverdeeld in 4 subcategorieën (SC): stembiljetten met enkel lijststemmen (SC1); stembiljetten voor alleen kandidaat-titularis(sen) (SC2); stembiljetten voor kandidaat-titularis(sen) en kandidaat-opvolger(s) (indien van toepassing) (SC3); stembiljetten voor alleen kandidaat-opvolger(s) (indien van toepassing) (SC4).

Les 4 tas sont examinés vote par vote et chaque vote est ajouté au parti, candidat ou suppléant choisi sur le formulaire prévu.

Après le dépouillement, on procède aux contrôles suivants :

• le nombre de votes enregistrés et la concordance entre les sous-catégories (SC) pour chaque liste: le nombre de bulletins de vote avec uniquement des votes en tête de liste (SC1); le nombre de bulletins de vote en faveur uniquement de candidat(s) titulaire(s) (SC2); le nombre de bulletins de vote en faveur de candidat(s) titulaire(s) et de candidat(s) suppléant(s) (si d'application) (SC3); le nombre de bulletins de vote uniquement en faveur de candidat(s) suppléant(s) (si d'application) (SC4); le chiffre électoral de la liste (CE)

• le chiffre électoral de la liste doit être égal à la somme des quatre sous-catégories (CE = SC1 + SC2 + SC3 + SC4).

• Pour les votes nominatifs: La somme des votes émis pour les candidats titulaires doit, en ce qui concerne cette liste, être égale au total des votes émis pour les candidats titulaires; La somme des votes émis pour les candidats suppléants doit, en ce qui concerne cette liste, être égale au total des votes émis pour les candidats suppléants; Le total des votes pour les titulaires doit être égal ou supérieur à la somme du total des bulletins de vote uniquement en faveur des titulaires (SC2) et du total des bulletins de vote pour les titulaires et suppléants (SC3); Le nombre total de vote pour les suppléants doit être égal ou supérieur à la somme du nombre total de bulletins de vote avec uniquement un vote en faveur des suppléants (SC4) et du nombre total de bulletins de vote en faveur des titulaires et des suppléants (SC3).

Ces procédures ne doivent pas être maintenues dans leur intégralité et peuvent être adaptées en fonction du système d'aide au dépouillement. Enfin, il faut établir un tableau par parti reprenant les 4 sous-catégories avec le nombre de votes de chaque candidat/suppléant.

B. Description du système

Le président du bureau de dépouillement reçoit un support de mémoire (par exemple une clef USB) reprenant tous les candidats. Au moyen d'une authentification (nom d'utilisateur et mot de passe), il télécharge le bon bureau de dépouillement avec les bons candidats. Ce support de mémoire est également utilisé comme output du système d'aide au dépouillement et comme input pour le système Martine (transmission des résultats au bureau principal). Ce support de mémoire doit donc être lisible sur la plupart des plateformes utilisables (notamment Windows). Le logiciel et le système d'exploitation (SE) peuvent être téléchargés avec l'interface ou sont déjà présents sur le système mais le fournisseur doit pouvoir offrir les garanties que la bonne version (contrôlée par un organisme d'avis agréé) du logiciel et du SE (y compris les drivers) doit être utilisée dans les bureaux de dépouillement. Comme output, cette interface doit comprendre les éléments suivants: Chaque vote individuel au format EML qui est signé de manière digitale; Les fichiers de résultats au format EML qui sont signés électroniquement; Le PV au format PDF qui est signé électroniquement.

Comme garantie complémentaire de l'intégrité du support de mémoire, un chiffre de contrôle est calculé sur les fichiers de résultats et ce chiffre s'affiche à l'écran du système d'aide au dépouillement. Ce chiffre de contrôle doit être repris sur le formulaire prévu à cette fin. Ce chiffre de contrôle est mentionné sur le PV avec un hash code sur l'ensemble des fichiers.

Les exigences de base demandées sont:

1. Prévoir un double encodage/comptage à titre de contrôle;

2. Les résultats des 2 encodages/comptages doivent être comparés, par comparaison des votes encodés/comptés. Si différence il y a, les bulletins sont vérifiés par l'ensemble du bureau et validés dans le système.

La numérotation des bulletins de vote est autorisée mais cette numérotation doit pouvoir être supprimée.

Une variante ne peut porter que sur la méthode de comparaison des votes entre les 2 encodages/comptages. Dans ce cas, toutes les spécifications techniques doivent être respectées.

C. Procédure de fabrication par l'autorité organisatrice

Pendant la procédure de fabrication des supports de mémoire, on peut utiliser du matériel de fabrication afin de fabriquer une interface master. Cette interface master est copiée en nombre suffisant afin de lancer les bureaux de dépouillement de manière sécurisée et distincte.

Cette procédure de fabrication doit pouvoir être exécutée simultanément pour tous les bureaux de dépouillement sur maximum 2 heures sans tenir compte des opérations humaines.

De 4 stapels worden stem per stem nagekeken en elke stem wordt toegevoegd bij de gekozen partij, kandidaat of opvolger op het voorziene formulier.

Na de telling gebeuren er volgende controles:

• het aantal opgenomen stemmen en de overeenkomst tussen de subcategorieën (SC) voor elke lijst: aantal stembiljetten met enkel lijststemmen (SC1); aantal stembiljetten voor alleen kandidaat-titularis(sen) (SC2); aantal stembiljetten voor kandidaat-titularis(sen) en kandidaat-opvolger(s) (indien van toepassing) (SC3); aantal stembiljetten voor alleen kandidaat-opvolger(s) (indien van toepassing) (SC4); stemcijfer van de lijst (CE)

• het stemcijfer van de lijst moet gelijk zijn aan de som van de vier subcategorieën (CE = SC1 + SC2 + SC3 + SC4).

• Voor de naamstemmen: De som van de uitgebrachte stemmen voor de kandidaat-titularissen moet, wat deze lijst betreft, gelijk zijn aan het totaal uitgebrachte stemmen voor de kandidaat-titularissen; De som van de uitgebrachte stemmen voor de kandidaat-opvolgers moet, wat deze lijst betreft, gelijk zijn aan het totaal uitgebrachte stemmen voor de kandidaat-opvolgers; Het totaal van de stemmen voor de titularissen moet gelijk zijn aan of groter zijn dan de som van het totaal van de stembiljetten voor enkel titularissen (SC2) en van het totaal aantal stembiljetten voor titularissen en opvolgers (SC3); Het totaal aantal stemmen voor opvolgers moet gelijk zijn aan of groter zijn dan de som van het totaal aantal stembiljetten met enkel een stem voor opvolgers (SC4) en van het totaal aantal stembiljetten voor titularissen en opvolgers (SC3).

Deze procedures moeten niet volledig behouden blijven en mogen worden aangepast in functie van het telhulpsysteem. Uiteindelijk moet er een tabel per partij met de 4 subcategorieën worden opgemaakt met het aantal stemmen van elke kandidaat/opvolger.

B. Beschrijving van het systeem

De voorzitter van het telbureau ontvangt een gegevensdrager (vb. USB-stick) met daarop alle kandidaten. Aan de hand van een authenticatie (username en wachtwoord) wordt het juiste telbureau met de juiste kandidaten opgeladen. Deze gegevensdrager wordt ook gebruikt als output van het telhulpsysteem en als input voor het systeem Martine (doorsturen van de resultaten in het hoofdbureau). Deze gegevensdrager moet dus leesbaar zijn op alle meest gebruikelijke platformen (o.a. Windows).De software en OS mag mee met de interface worden opgeladen of reeds aanwezig zijn op het systeem zelf, maar de leverancier moet garanties kunnen geven dat de juiste versie (gecontroleerd door een erkend adviesorgaan) van de software en OS (incl. drivers) gebruikt wordt in de telbureaus. Als output moet deze interface het volgende bevatten: Elke individuele stem in EML-formaat dat digitaal ondertekend is; De resultatenbestanden in EML-formaat die digitaal ondertekend zijn; Het PV in pdf-formaat dat digitaal ondertekend is

Als bijkomende integriteitsgarantie van de gegevensdrager wordt er een controlegetal berekend op de resultatenbestanden en wordt dit weergegeven op het scherm van het telhulpsysteem. Dit controlegetal moet worden overgenomen op het daartoe voorziene formulier. Dit controlegetal wordt samen met een hashcode op het geheel van de bestanden opgenomen in het PV.

Als basisvereiste wordt er gevraagd om:

1. een dubbele input/telling te voorzien als controle;

2. de resultaten van de 2 inputs/tellingen te vergelijken met de geregistreerde/getelde stemmen. Indien er een verschil is, worden de stembiljetten door het hele bureau gecontroleerd en gevalideerd in het systeem.

Het nummeren van de stembiljetten is toegelaten, maar deze nummering moet opnieuw kunnen verwijderd worden.

Een variante mag enkel betrekking hebben op de methode voor vergelijking van de stemmen tussen de 2 inputs/tellingen. Alle voorschriften van het bestek moeten nageleefd worden.

C. Aanmaakprocedure door de organiserende overheid

Tijdens de aanmaakprocedure van de gegevensdragers kan er gebruik gemaakt worden van aanmaakapparatuur om één master interface aan te maken. Deze master interface wordt gekopieerd in voldoende aantal om alle telbureaus beveiligd en afzonderlijk te kunnen opstarten.

Deze aanmaakprocedure moet voor alle telbureaus tezamen kunnen uitgevoerd worden op maximaal 2 uur geen rekening gehouden met menselijke handelingen.

Toutes les données d'import, telles que les bureaux de dépouillement et les listes de candidats, doivent pouvoir être chargées en batch.

Le processus de production prévoit la préparation et l'utilisation d'une infrastructure à clé publique (PKI) pour générer des clés cryptographiques pour les bureaux de dépouillement. Par système de comptage une paire de clés unique sera créée avec un certificat. Sur la base de ces ICP, il devrait être possible de vérifier l'intégrité des résultats numériques des centres de comptage.

Les conditions suivantes doivent être remplies ici:

1) Le PKI (hardware, logiciels et procédures) sera livré dans le cadre du processus de création, et est seulement sous contrôle (et utilisé sur les systèmes) des autorités organisatrices.

2) Les clés privées sont chiffrées par le système d'aide au dépouillement et stockées sur le support de mémoire « maître ». Celles-ci ne peuvent être déchiffrées et utilisées dans les centres de dépouillement que via un mot de passe distinct pour le bureau de totalisation, qui est transmis d'une manière différente (par exemple sous enveloppe scellée).

3) Le système de comptage utilise ces clés cryptographiques afin de signer les résultats de comptage numérique, de sorte qu'il doit être possible de vérifier l'intégrité et l'authenticité des résultats de comptage.

4) La solution fournit également un rapport de certification (CA) qui valide les résultats de comptage signés numériquement (en format PDF et / ou le format EML).

5) La procédure d'accompagnement fournit des instructions claires sur la façon dont la clé privée de la racine et / ou sous-CA doit être établie (entre autres hors ligne de stockage et de sauvegarde de celui-ci).

6) La solution proposée utilise des normes telles que les certificats X.509 et les algorithmes cryptographiques publiquement connus et fiables, par exemple. RSA ou ECC pour cryptages.

D. Compatibilité

Le système est compatible avec le système pour la totalisation et la transmission des résultats (Martine).

En output chaque système de comptage présente les caractéristiques suivantes:

- Chaque voix individuelle au format EML qui est signé numériquement

- Les fichiers de résultats au format EML qui ont été signés numériquement

- Le PV en format pdf qui a été signé numériquement

Le rapport avec les résultats doivent être signés numériquement avec la clé privée du système d'aide au dépouillement (nécessite des clés uniques par bureau de totalisation présentes dans l'interface maître).

E. Législation

Le système doit toujours satisfaire à la législation électorale et à la législation linguistique.

Le système doit être politiquement neutre. L'utilisation de couleurs est autorisée mais l'administration peut toujours demander d'adapter gratuitement le lay-out.

L'exactitude de la langue et l'emploi de la bonne langue dans chaque région doivent être respectés, en particulier dans les communes à facilités.

F. Exigences non fonctionnelles

L'application doit non seulement être conviviale mais elle doit également satisfaire aux exigences de sécurité les plus récentes.

Convivialité et performance

* Un système d'aide au dépouillement doit pouvoir être monté et démonté dans les 10 minutes. Cela comprend le temps nécessaire pour sortir le système de son emballage et le réemballer.

* Le système d'aide au dépouillement doit pouvoir être démarré jusqu'à l'écran de connexion dans un délai d'une minute.

* Le système d'aide au dépouillement doit lire et traiter la configuration de la clef USB jusqu'à l'écran d'accueil de l'application dans un délai de 1 minute. Son avancement doit pouvoir être suivi visuellement.

* L'application doit être ergonomique et son utilisation doit être facile et logique.

Alle importgegevens, zoals de telbureaus en de kandidatenlijsten, moeten in batch kunnen verwerkt worden.

De aanmaakprocedure voorziet in de aanmaak en het gebruik van een Public Key Infrastructuur (PKI) om cryptografische sleutels te genereren voor de telbureaus. Per telsysteem zal een uniek sleutelpaar gemaakt worden, samen met een certificaat. Op basis van deze PKI moet het mogelijk zijn om de integriteit van de digitale resultaten van de telbureaus te controleren.

De volgende vereisten moeten hierbij ingevuld worden:

1) De PKI (hardware, software en procedures) wordt opgeleverd als onderdeel van de aanmaakprocedure en wordt enkel onder controle (en op systemen) van de organiserende overheid gebruikt.

2) De private sleutels per telhulpsysteem worden versleuteld opgeslagen op de master gegevensdrager. Deze kunnen enkel gedecrypteerd en gebruikt worden in de telbureaus. Hiervoor wordt een apart paswoord per telbureau gemaakt, dat op een aparte manier wordt doorgestuurd (bv. Een verzegelde enveloppe).

3) Het telsysteem gebruikt deze cryptografische sleutels om de telresultaten digitaal te tekenen, waardoor het mogelijk moet zijn om de integriteit en authenticiteit van de telresultaten te controleren.

4) De oplossing levert ook een Certificate Authority (CA), waarmee digitaal getekende telresultaten (in PDF en/of EML formaat) gevalideerd worden.

5) De bijgeleverde procedure voorziet in duidelijke instructies hoe de private sleutel van de root en/of sub-CA moet beveiligd worden (o.a. off-line opslag en back-up hiervan).

6) De voorgestelde oplossing maakt gebruikt van standaarden zoals bv. X.509 voor de certificaten en publiek gekende en betrouwbare cryptografische algoritmes zoals bv. RSA of ECC voor de versleutelingen.

D. Compatibiliteit

Het systeem is compatibel met het systeem voor de totalisatie en het doorsturen van de resultaten (Martine).

Als output moet elk telsysteem het volgende voorzien:

- Elke individuele stem in EML-formaat dat digitaal ondertekend is

- De resultatenbestanden in EML-formaat die digitaal ondertekend zijn

- Het PV in pdf-formaat dat digitaal ondertekend is

Het digitale verslag met de resultaten moeten digitaal getekend worden met de private sleutel van het telhulpsysteem (hiervoor zijn unieke sleutels per telbureau aanwezig op de master interface).

E. Wetgeving

Het systeem moet steeds voldoen aan de kieswetgeving en de taalwetgeving.

Het systeem moet politiek neutraal zijn. Het gebruik van kleuren is toegelaten, maar de administratie mag steeds vragen om de lay-out gratis bij te sturen.

De correctheid van de taal en het gebruik van de juiste taal in elke regio moet gerespecteerd worden, in het bijzonder in de gemeenten met faciliteiten.

F. Niet-Functionele Vereisten

Niet alleen moet de toepassing gebruiksvriendelijk zijn en voldoen aan de recentste veiligheidsvereisten.

Gebruiksvriendelijkheid en performantie

* Eén telhulpsysteem moet door 1 persoon binnen 10 minuten opgesteld en afgebouwd kunnen worden. Dit is inclusief de tijd die nodig is om het systeem uit de verpakking te halen en weer in te pakken.

* Het telhulpsysteem moet binnen 1 minuut opgestart zijn tot het inlogscherm.

* Het telhulpsysteem moet de configuratie van de USB stick binnen de 1 minuut inlezen en verwerken tot het startscherm van de applicatie. De vooruitgang hiervan dient visueel te volgen zijn.

* De toepassing moeten ergonomisch zijn en eenvoudig en logisch zijn in gebruik.

* Les applications fournies doivent être intuitives et doivent pouvoir être utilisées sans aide.

* Lorsque l'on clique sur les différents champs à compléter, un texte explicatif s'affiche automatiquement.

* Pour les mentions du système d'aide au développement s'appliquent les conditions suivantes :

o Les mentions du statut doivent être visuelles.

o Les messages d'erreurs doivent être formulés en étapes de procédure claires afin que l'utilisateur sache ce qu'il faut faire.

o La mention doit clairement préciser si un problème peut être résolu grâce à une action du bureau de dépouillement ou si un helpdesk doit intervenir.

o Le message doit clairement indiquer le degré d'urgence, en utilisant des couleurs par exemple.

* Les temps de réponse du système d'aide au dépouillement sont de:

o Maximum 0,1 seconde lors de la manipulation d'un objet dans un écran.

o Maximum 1 seconde lors du passage à l'étape suivante du processus de dépouillement.

* Le système d'aide au dépouillement doit effacer les résultats de la clef USB dans un délai de 5 minutes. Sa progression doit être suivie visuellement.

Sécurité

De manière générale, le fournisseur prévoit les mesures de sécurité nécessaires afin de prévenir, détecter et atténuer des incidents de sécurité.

Organisation

* Le fournisseur travaille sur la base d'un cadre de la sécurité des informations qu'il doit mentionner (basé sur ISO27K, COBIT ou une norme internationale comparable). Ce cadre définit notamment les rôles et les responsabilités, les mesures de sécurité et les procédures.

* Le fournisseur dispose d'un plan de réaction en cas d'incident afin de réagir adéquatement en cas d'incidents de sécurité (en fonction de la classification de l'incident) y compris une analyse de cause racine et le développement de solutions durables.

* Le fournisseur a un responsable de la sécurité de l'information qui assure la conformité du cadre de la sécurité de l'information et des aspects sécurité de tous les produits livrables.

* Il y a lieu de réaliser une recherche d'antécédents appropriée pour tous les collaborateurs du fournisseur impliqués dans le traitement des données du projet. Le fournisseur garantit l'intégrité de ses collaborateurs et sous-traitants éventuels et il garantit que tous les collaborateurs ont suivi des formations en sécurité adéquates.

* Le fournisseur désigne un délégué à la protection des données (data protection officer) afin de garantir la protection des données.

* Le fournisseur dispose d'un cadre de développement sûr et démontrable qu'il doit mentionner (basé sur OWASP SAMM, BSIMM ou une meilleure pratique internationale comparable) pour le développement et l'exploitation opérationnelle du logiciel fiable.

Développement du logiciel

* Les vulnérabilités du logiciel sont identifiées et corrigées le plus tôt possible au cours du cycle de développement.

* On utilise un processus d'élaboration de logiciel fiable, à mentionner, qui compile le logiciel fourni et l'associe à tous les fichiers sources. Cela comprend une méthode de vérification de l'intégrité du logiciel.

* On utilise des environnements strictement distincts pour le développement, les tests, l'acceptance, la formation et la production.

* Le logiciel fourni ne contient aucun code malveillant tel que des virus informatiques, des vers, des bombes à retardement, des trappes, des chevaux de Troie ou des œufs de Pâques.

* Le fournisseur développera et documentera, dans le cadre d'une phase d'analyse, des exigences de sécurité détaillées pour le logiciel. Celles-ci décriront les mécanismes de sécurité et des

* De geleverde toepassingen moeten intuïtief zonder extra hulp kunnen worden gebruikt.

* Bij de verschillende velden die moeten ingevuld worden, wordt er automatisch een begeleidende tekst weergegeven wanneer hierop geklikt wordt.

* Voor meldingen van het stemhulpsysteem geldt:

o Statusmeldingen moeten visueel worden weergegeven.

o Foutmeldingen moeten worden geformuleerd in begrijpelijke processtappen zodat de gebruiker weet wat er moet gebeuren.

o Uit de melding moet eenduidig blijken of een probleem door een handeling van het telbureau is te verhelpen dan wel dat een helpdesk moet worden ingeschakeld.

o De urgentie moet eenduidig uit de melding blijken, bijvoorbeeld door kleuren te gebruiken.

* De responsetijden van het telhulpsysteem zijn:

o Maximum 0,1 seconde bij manipulatie van een object in een scherm.

o Maximum 1 seconde bij de overgang naar een volgende stap in het telproces.

* Het telhulpsysteem moet de uitslagen op de USB stick binnen de 5 minuten wegschrijven. De vooruitgang hiervan dient visueel te volgen zijn.

Beveiliging

Algemeen voorziet de aanbieder de nodige beveiligingsmaatregels om beveiligingsincidenten te voorkomen, detecteren en mitigeren.

Organisatie

* De leverancier werkt op basis van een te vermelden informatiebeveiligingsraamwerk (gebaseerd op ISO27K, COBIT of een vergelijkbare internationale standaard). Dit raamwerk definieert onder meer de rollen & verantwoordelijkheden, beveiligingsmaatregelen en procedures.

* De leverancier heeft een incident response plan om adequaat op beveiligingsincidenten te reageren (in functie van incident classificatie) inclusief root-cause analyse en het uitwerken van duurzame oplossingen.

* De leverancier heeft een informatiebeveiligingsverantwoordelijke die de compliance van het informatiebeveiligingsraamwerk en de beveiligingsaspecten van alle deliverables verzekert.

* Passende antecedentenonderzoek moet worden uitgevoerd voor alle medewerkers van de leverancier die betrokken zijn bij de verwerking van de project gegevens. De leverancier garandeert de integriteit van zijn medewerkers en eventuele onderaannemers, en garandeert dat alle medewerkers adequate beveiligingsopleidingen gevolgd hebben.

* Een data protectie officer wordt aangesteld door de leverancier om de gegevensbescherming te waarborgen.

* De leverancier heeft een te vermelden aantoonbaar veilig ontwikkel raamwerk (gebaseerd op OWASP SAMM, BSIMM of een vergelijkbare internationale best practice) voor de ontwikkeling en operationele uitbating van betrouwbare software.

Softwareontwikkeling

* Software kwetsbaarheden worden zo vroeg mogelijk tijdens de ontwikkelcyclus geïdentificeerd en opgelost.

* Een te vermelden betrouwbaar software buildproces wordt gebruikt die de geleverde software compileert en linkt van alle bronbestanden. Dit omvat een methode voor het verifiëren van de integriteit van de software.

* Strikt gescheiden omgevingen worden gebruikt voor ontwikkeling, testen, acceptatie, opleiding en productie.

* De geleverde software bevat geen kwaadaardige code, zoals viruses, worms, time bombs, back doors, Trojan horses of Easter eggs.

* De leverancier zal - als onderdeel van een analyse fase - gedetailleerde beveiligingsvereisten voor de software uitwerken en documenteren. Deze zullen de beveiligingsmechanismes en

patrons de conception sûrs ainsi que la manière dont ceux-ci seront implémentés dans la solution proposée.

* Les composantes logicielles de tierces parties qui seront utilisées (y compris le logiciel open source) devront satisfaire à ces exigences.

* Le SE est durci selon les dernières meilleures pratiques du fournisseur du SE :

o L'intégrité du SE est garantie par l'utilisation d'un Trusted Platform Module (TPM) sur le matériel utilisé.

o Le logiciel minimum est installé et tous les logiciels ou modules inutiles et les exemples de fichiers sont supprimés.

o Seuls les services ou daemons nécessaires sont installés.

o Les certificats standards sont remplacés.

* Tous les logiciels livrés (y compris le SE et le logiciel de tierces parties) sont régulièrement mis à niveau en utilisant les versions les plus récentes afin de résoudre ou de prévenir les vulnérabilités. Les administrations sont toujours informées lorsque certaines modifications sont nécessaires et elles reçoivent une description détaillée du risque et de la solution proposée.

* L'application génère un journal de sécurité et celui-ci est enregistré au niveau local et sur la clef USB.

* Le Security logging comprend au minimum les éléments suivants :

o Heure (exprimée en UTC)

o Nom système des systèmes concernés

o Identité de l'utilisateur

o Severity level

o Détail de l'évènement.

* Les évènements de sécurité suivants doivent au moins être consignés dans un journal de sécurité :

o Login – logout réussi/raté

o Exceptions dans les applications

* Les journaux de sécurité doivent être conservés jusqu'à l'approbation officielle des élections par l'instance compétente.

Tests de sécurité du logiciel

Le fournisseur prévoira au moins les tests suivants comme élément du processus de développement sécurisé pour le logiciel fourni:

* Les tests de sécurité doivent tester le bon fonctionnement des exigences de sécurité ainsi que l'absence de vulnérabilités très fréquentes (comme le Top 10 OWASP).

* Les tests de sécurité doivent notamment inclure des tests de sécurité statiques et dynamiques. Le résultat de ces tests ainsi qu'une description dans un rapport de test doivent être fournis avec chaque version du logiciel électoral.

* Les tests de sécurité sont toujours une composante des tests d'acceptance pour ce cahier spécial des charges. Le logiciel électoral fourni ne peut être accepté que si toutes les vulnérabilités en matière de sécurité ont été résolues ou acceptées comme risques par les pouvoirs adjudicateurs.

* Le pouvoir adjudicateur a toujours le droit de soumettre le logiciel fourni à des tests de sécurité réalisés par une tierce partie. A cette fin, le fournisseur mettra le support nécessaire à la disposition de la tierce partie (par exemple mettre à disposition le code source ou l'environnement de test et donner les renseignements nécessaires).

Matériel sécurisé

*Le fournisseur doit utiliser du matériel d'un fournisseur fiable.

* Le matériel utilisé doit être équipé d'un Trusted Platform Module (TPM) fonctionnel qui satisfait aux exigences les plus récentes du Trusted Computing Group[1] (TCG).

* Soit le matériel utilisé est utilisé une seule fois pour les élections et ensuite (après une procédure d'effacement sécurisée) réutilisé à d'autres fins pour le fournisseur. Soit le fournisseur stockera le matériel de manière sécurisée entre les élections (jusqu'à la fin de la durée du contrat).

veilig design patterns beschrijven en hoe deze in de aangeboden oplossing worden geïmplementeerd.

* Gebruikte software componenten van derde partijen (inclusief open source software) moeten ook aan deze vereisten voldoen.

* De OS wordt hardened volgens de laatste best-practices van de OS leverancier:

o De integriteit van het OS wordt gegarandeerd door het gebruik van Trusted Platform Module (TPM) op de gebruikte hardware.

o De minimum software wordt geïnstalleerd, en alle onnodige software of modules en voorbeeld bestanden worden verwijderd.

o Alleen de nodige services of daemons worden opgezet

o De standaard credentials worden veranderd

* Alle geleverde software (inclusief OS en software van derde partijen) zullen op regelmatige basis up to date gebracht worden naar de meest recente versies om kwetsbaarheden op te lossen of te voorkomen. De administraties worden steeds op de hoogte gesteld wanneer bepaalde wijzigingen noodzakelijk zijn en krijgen een gedetailleerde beschrijving van het risico en de voorgestelde oplossing.

* Vanuit de applicatie wordt een security log gegenereerd en opgeslagen lokaal en op de USB stick.

* Security logging omvat minimaal volgende elementen:

o Tijdstip (in UTC)

o systeem naam van de betrokken systemen

o Identiteit gebruiker

o Severity level

o Detail van het event.

* Volgende security events moeten minimaal gelogd worden in een security log:

o Succesvol /mislukte login – logout

o Uitzonderingen (exceptions) in de applicaties

* Security logs moeten bewaard worden tot de verkiezingen officieel zijn goedgekeurd door de bevoegde instantie.

Testen veilige software

De leverancier zal minstens volgende testen voorzien als onderdeel van een veilig ontwikkelproces voor de geleverde software:

* De beveiligingstesten moeten een correcte werking van de beveiligingsvereisten testen alsook het ontbreken van veel voorkomende software gebreken.

* De beveiligingstesten moeten onder meer statische en dynamische beveiligingstesten omvatten. De uitkomst van deze testen moet samen met een beschrijving in een testrapport, meegeleverd worden bij elke release van de software.

* Beveiligingstesten zijn steeds onderdeel van de acceptatie testen voor dit bestek. De geleverde software kan enkel geaccepteerd worden als alle gevonden beveiligingskwetsbaarheden zijn opgelost of door de opdrachtgevers aanvaard als risico's.

* De opdrachtgever heeft steeds het recht om de geleverde software te onderwerpen aan beveiligingstesten door een derde partij. De leverancier zal hiervoor de nodige ondersteuning beschikbaar maken aan de derde partij (bv. beschikbaar maken van de source code of een test omgeving en het geven van de nodige toelichtingen).

Veilige hardware

* De leverancier moet hardware gebruiken van een betrouwbare leverancier.

* De gebruikte hardware moet uitgerust zijn met een ingeschakelde Trusted Platform Module (TPM) dat voldoet aan de meest recente vereisten van de Trusted Computing Group[1] (TCG).

* Ofwel wordt de gebruikte hardware éénmalig gebruikt voor de verkiezingen en nadien (na een veilig wisproces) hergebruikt voor andere doeleinden van de leverancier. Ofwel zal de leverancier de hardware zelf beveiligd opslaan tussen de verkiezingen (tot aan het einde van de looptijd van het contract).

* Le matériel est transporté dans les bureaux de dépouillement uniquement par transport sécurisé et traçable.

* Le matériel pour le système d'aide au dépouillement est livré dans une caisse de transport fermée et scellée dans laquelle les éléments sont transportés et stockés. Dans celle-ci se trouve également les scellés ainsi que les instructions pour le faire enlever par le fournisseur.

* Le fournisseur se charge du stockage sécurisé du matériel, les mesures suivantes doivent être prises:

o L'extérieur du lieu ou du bâtiment est suffisamment solide et suffisamment protégé contre l'accès par des personnes non autorisées (par exemple une clôture solide, des murs extérieurs, des portes extérieures, des fenêtres extérieures, ...).

o L'accès au bâtiment et à l'espace de stockage est contrôlé afin que seules les personnes autorisées aient accès (par exemple: surveillance permanente, une réception avec du personnel, système de badge, ...).

o Un nombre limité de collaborateurs autorisés a accès à l'espace de stockage.

o Il y a un contrôle d'accès et un logging sur la base de badges d'accès électroniques. Le logging est conservé au moins 3 mois.

o Des systèmes antieffraction adaptés sont installés et le fonctionnement effectif de ceux-ci est testé à intervalles réguliers.

o L'espace de stockage est pourvu d'un contrôle caméra. Les images en sont conservées au moins 1 mois.

o Les journaux d'accès et les images caméra peuvent être contrôlés par une tierce partie.

Maintenabilité

* Pendant les développements, on vérifie toujours si la qualité du code satisfait à la norme de maintenabilité conformément aux définitions dans ISO25010.

* Les langues de programmation qui sont principalement utilisées sont faites d'une combinaison courante de technologies telles que les technologies javastack , C# stack et HTML5.

* Le logiciel a un code source bien structuré et est scindé en modules. Chaque module contient le commentaire nécessaire en anglais qui en explique le fonctionnement.

* Les unités de code source (classes, méthodes) sont petites ce qui limite le nombre de constructeurs.

* La fonctionnalité est écrite une seule fois et réutilisée dans le logiciel (aucun copier/coller de code).

* Les interfaces dans le code sont limitées et claires.

* La couverture de test par unité est démontrable à > 80 % grâce à un outil d'analyse statique, mesurée comme la couverture des ramifications du programme (nombre de chemins décisionnels testés). On prévoit suffisamment de tests d'unité, de sorte que des adaptations peuvent, si nécessaire, être apportées rapidement.

* On n'utilise pas de bibliothèques obsolètes ou de bibliothèques pour lesquelles des vulnérabilités ont été constatées. Pour prévenir ceci, un processus actif de gestion des correctifs est nécessaire.

Art. 3. Le présent arrêté entre vigueur le jour de sa publication au *Moniteur belge*.

Bruxelles, le 4 mars 2019.

P. DE CREM

Note

1 https://trustedcomputinggroup.org

* Hardware wordt enkel met beveiligd en traceerbaar transport geleverd en opgehaald in de telbureaus.

* De hardware voor het telhulpsysteem wordt geleverd in een afgesloten en verzegelde transportbehuizing waarin de onderdelen vervoerd en opgeslagen worden. Hierin zitten ook de verzegeling en de instructies om dit te laten ophalen door de leverancier.

* De leverancier zorgt voor een veilige opslag van de hardware, hierbij worden de volgende maatregelen getroffen:

o De buitenkant van de locatie of het gebouw is voldoende solide en op voldoende wijze beschermd tegen toegang door onbevoegden (vb. solide omheining, buitenmuren, buitendeuren, buitenramen, ...).

o De toegang tot het gebouw en tot de opslagruimte wordt gecontroleerd zodanig dat enkel bevoegde personen toegang krijgen (vb. permanente bewaking, bemande receptie, badgesysteem, ...).

o Een beperkt aantal bevoegde medewerkers heeft fysiek toegang tot de opslagruimte.

o Er is toegangscontrole en logging op basis van elektronische toegangspassen. Logging hiervan wordt minstens 3 maanden bijgehouden.

o Er zijn gepaste anti-inbraaksystemen geïnstalleerd waarvan de effectieve werking op regelmatige tijdstippen getest wordt.

o Er is camera controle op de opslagruimte. Hiervan worden de beelden minstens 1 maand bijgehouden.

o De toegangslogs en camerabeelden kunnen door een 3e partij gecontroleerd worden.

Onderhoudbaarheid

* Tijdens de ontwikkelingen wordt er steeds afgetoetst of codekwaliteit meetbaar voldoet aan de norm voor onderhoudbaarheid conform de definities in ISO25010.

* De gebruikte programmeertalen zijn een gangbare combinatie van Swift, Java, JavaScript, C# en/of HTML5.

* De software heeft een goed gestructureerde en duidelijk leesbare broncode. Elke module bevat de nodige commentaar in het Engels die de werking ervan verduidelijkt.

* De broncode units (klassen, methodes) zijn klein waarbij het aantal constructors beperkt is.

* Functionaliteit wordt één keer geschreven en binnen de software hergebruikt (geen copy/paste van code).

* Interfaces in de code zijn beperkt en duidelijk.

* Unit-testdekking is met statische analysetooling aantoonbaar > 80 %, gemeten als branch-coverage (aantal beslispaden dat is getest). Er worden voldoende unittesten voorzien, zodat indien nodig in een vroege fase kan worden bijgestuurd.

* Er worden geen verouderde libraries gebruikt of libraries waarbij er zwakheden zijn vastgesteld. Om dat te borgen is een actief patchmanagement proces noodzakelijk.

Art. 3. Dit besluit treedt in werking op de dag dat het in het *Belgisch Staatsblad* bekendgemaakt wordt.

Brussel, 4 maart 2019.

P. DE CREM

Nota

1 https://trustedcomputinggroup.org