MASTER EN SCIENCES INFORMATIQUES

Analyse du vote électronique par internet pour des élections corporatistes

Maréchal, Michaël

Award date:
2009

Facultés Universitaires Notre Dame de la Paix, Namur
Faculté d'Informatique
Année académique 2008-2009

ANALYSE DU VOTE ELECTRONIQUE PAR INTERNET POUR DES ELECTIONS CORPORATISTES

Michaël Maréchal

Mémoire présenté en vue de l'obtention du grade de licencié en informatique

Résumé

Les nouvelles technologies sont présentes partout ou presque dans notre vie quotidienne. Le système électoral n'échappe pas à ce phénomène même si certaines associations demandent le retour au bulletin papier.

D'abondantes recherches, toujours en cours aujourd'hui, se focalisent sur l'évaluation des possibilités d'un vote électronique (e-voting) voire d'un vote électronique à distance par Internet (i-voting). Qu'en est-il des risques ? Peut-on faire confiance aux systèmes proposés actuellement ? L'électeur contrôle-t-il encore ce processus électoral ?

Cet ouvrage tente d'analyser les risques encourus par des élections corporatistes utilisant Internet et d'illustrer ces systèmes électoraux à l'aide de modèles.

Ce travail s'articule autour du contrôle de l'électeur sur l'ensemble du processus électoral et autour du respect des règles en vigueur pour des élections corporatistes.

En conclusion, des solutions peuvent être proposées à l'électeur quant à la vérifiabilité de l'élection. En parallèle, l'usage d'Internet pour les élections corporatistes entraîne certains risques : certains peuvent être mis sous contrôle, d'autres restent préoccupants pour la tenue de scrutin par Internet.

Abstract

New technologies are present almost everywhere in our daily lives. The electoral system is not immune to this phenomenon, although some associations request a return to paper ballots.

Abundant research still going on today, focus on assessing the feasibility of electronic voting (e-voting) or even a distant electronic voting via the Internet (i-voting). What are the risks? Can we trust the systems currently available? Can the voter still control the election process?

This work attempts to analyse the risks of using Internet corporatist elections and illustrate these electoral systems with models.

This work revolves around the control of the voter of the whole electoral process and the respect of the rules for corporatist elections.

In conclusion, solutions can be proposed to the voter for the feasibility of the election. In parallel, the use of the Internet for corporatist elections entail certain risks: some may be controlled, others remain a concern for the voting by Internet.

Remerciements

J'aimerais humblement remercier certaines personnes qui ont participé, de près ou de loin, à l'élaboration de ce mémoire et sans lesquelles ce projet n'aurait jamais vu le jour.

Tout d'abord, je tiens à remercier les professeurs, Monsieur Ramaekers et Monsieur Schumacher, pour leur disponibilité, leur expérience et les nombreuses références intéressantes transmises.

Ensuite, je voudrais remercier les différents experts que j'ai contactés, dans le monde de l'informatique et dans le monde des élections corporatistes.

Enfin, je dédie un « MERCI » tout particulier à mes proches qui m'ont soutenu et encouragé tout au long de ces études en horaire décalé.

Encore merci aux personnes qui ont consacré un peu de leur temps pour la relecture de ce mémoire de fin d'études.

Table des matières

Table des figures

Glossaire

OSCE
L'Organisation pour la Sécurité et la Coopération en Europe regroupe 56 états situés en Europe, en Asie centrale et en Amérique. L'OSCE offre à tous les états participants un forum pour les négociations politiques.
Le Bureau pour les Institutions Démocratiques et les Droits de l'Homme (ODIHR – Office for Democratic Institutions and Human Rights) est régulièrement observateur pour les élections.
[Organisation pour la sécurité et la coopération en Europe] [Office for Democratic Institutions and Human Rights, 2007]

Suffrage libre
Libre formation et expression de l'opinion de l'électeur. [Comité des Ministres du Conseil de l'Europe, 2004]

Suffrage équitable
Suffrage durant lequel l'électeur ne peut déposer qu'un seul bulletin dans l'urne.
[Comité des Ministres du Conseil de l'Europe, 2004]

Processus électoral
Ensemble des étapes nécessaires pour la réalisation du vote démocratique comprenant notamment l'inscription des électeurs, l'inscription des candidats, le vote, le dépouillement et la proclamation des résultats.

Électeur
Personne habilitée à exprimer un suffrage dans une élection ou un référendum donné
[Comité des Ministres du Conseil de l'Europe, 2004]

CBFA
La Commission Bancaire, Financière et des Assurances contrôle les établissements financiers, les marchés financiers, lutte contre le blanchiment d'argent, ...
[CBFA]

Febelfin
La Febelfin est la fédération-coupole du secteur financier belge. Elle joue un rôle de conciliateurs entre ses membres et différentes parties au niveau national et européen : fédérations professionnelles, décideurs politiques, autorités de contrôle.
[Febelfin]

Introduction

Le vote par Internet, ou i-vote, fait l'objet de nombreux projets de recherche et d'expériences grandeur nature de par le monde depuis plusieurs années. Différents buts sont poursuivis, certains visant très directement à simplifier les opérations de vote

- Rapidité de dépouillement
- Diminution du nombre de bulletins nuls
- Facilitation du vote des personnes à mobilité réduite et/ou en déplacement

d'autres plus sociétaux

- Amélioration du taux de participation
- Augmentation de l'intérêt des citoyens pour la chose publique
- Image de marque de la Société, à la pointe de la technologie

Dans certains domaines (élections sociales, élections estudiantines, etc), Internet est (ou sera prochainement) régulièrement utilisé pour la collecte des votes. Cependant, dans les domaines qui touchent plus fortement à la démocratie, comme les élections législatives d'un pays, l'usage d'Internet est loin d'être généralisé. Pour expliquer ce constat, d'aucuns évoquent l'incompréhension du processus par une grosse partie de la population, le manque apparent de transparence des opérations et la confiscation du contrôle citoyen par les experts. En Belgique, l'association PourEVA constate que le contrôle des opérations électorales n'est plus dans les mains du citoyen mais bien de techniciens spécialisés. Pour cette association, composée principalement d'informaticiens, le vote automatisé remet également en question la garantie du secret du vote. [PourEVA, 2007]

Objectif du mémoire

Afin d'arriver à susciter la confiance dans les procédures de vote automatisées, il importe de proposer des solutions permettant aux citoyens de contrôler chaque étape du processus électoral mais également d'avoir la certitude que le système respecte une série de règles. C'est à ces tâches que le présent mémoire s'attache, dans le cas du vote électronique par Internet, ou I-vote, mis en oeuvre pour des élections corporatistes.

Plan du mémoire

Pour commencer, le chapitre 1 établira une nomenclature des solutions de vote électronique. Une brève évocation d'autres systèmes de vote sera proposée, avant de cerner notre propos au vote électronique par Internet.
Ensuite, le chapitre 2 s'attachera plus particulièrement aux élections corporatistes. Le terme "élections corporatistes" sera défini par quelques exemples concrets. Le processus électoral de chacun de ces exemples sera détaillé. Les ressemblances entre ces différents processus seront mises en évidence, afin de se consacrer principalement aux étapes de vote et de dépouillement.
Le chapitre suivant réalisera l'analyse de risques de ces étapes identifiées au chapitre 2. Pour mener à bien cette analyse, il nous faudra d'abord définir la notion de "risques". Nous introduirons comme référentiel d'analyse les recommandations du Conseil de l'Europe, qui servent actuellement de normes à respecter pour les élections démocratiques dans les 27 pays membres. D'autres exigences de sécurité seront également abordées.
Avant de conclure, le chapitre 4 proposera une modélisation des systèmes étudiés, permettant une comparaison plus aisée de ceux-ci.
Enfin une conclusion clora ce mémoire.

1 Nomenclature du vote automatisé

Dans un scénario de gouvernement représentatif, les élections, quelles que soient leurs modalités, sont le mécanisme par lequel les membres d'un groupe, d'une communauté élisent leurs représentants pour exercer, en leur nom, une fonction politique, économique ou sociale. De nos jours, les élections sont organisées dans de nombreuses organisations pour en désigner les responsables : entreprises (conseil d'administration, conseil d'entreprise, CPPT), partis politiques, sociétés savantes, etc.
Si le concept d'élection est vieux comme le monde, la manière d'organiser les élections a évolué dans le temps. L'une des évolutions majeures de ce domaine dans les dernières décennies fut l'émergence de l'automatisation du processus électoral. L'on pense ici aux machines à voter mécaniques utilisées dans de nombreux pays, à leurs évolutions électroniques, ou encore, depuis une quinzaine d'années, aux élections organisées via Internet.
Dans la suite du chapitre, nous allons proposer une nomenclature de ces procédures du vote, illustrée par de nombreux exemples.

1.1 Vote automatisé

En Belgique, le concept de "vote automatisé" est utilisé par l'association militante "PourEVA" pour désigner les alternatives au vote manuel sur support papier. Dans le présent mémoire, ce concept est généralisé à toute procédure reposant sur le recours à un équipement mécanique. Les systèmes électroniques font l'objet d'une autre section.
Au nombre de ces systèmes de vote automatisé, l'on compte donc les machines à voter mécaniques utilisées dans de nombreux pays, par exemple aux Etats-Unis, où les ratés de la procédure de vote de l'état de Floride ont défrayé la chronique en 2000.

1.2 Vote électronique ou e-vote

Dans le scénario du "vote électronique" ou e-vote tel que nous l'entendons, la machine à voter mécanique de la section précédente est remplacée par un équipement électronique, un ordinateur par exemple, mais le centre de récolte des votes exprimés sur cette machine est placé dans le même local que la dite machine. Au moment du vote, l'électeur, la machine et le centre de collecte sont co-localisés. Il n'y a donc pas de recours à une infrastructure publique de communication entre eux.
C'est typiquement le scénario utilisé aux dernières élections régionales et européennes en Belgique où, dans 34% des communes (ou 49% des électeurs), l'électeur, placé face à un écran, émet son vote à l'aide d'un crayon optique. Son vote est enregistré sur une carte magnétique qui est ensuite déposée dans une urne. Le dépouillement et le décompte des voix se font automatiquement par lecture des cartes magnétiques.
[Service Public Fédéral Belge, 2008]

Les modalités techniques d'un vote électronique peuvent faire l'objet de nombreux ajustements. Dans le rapport remis en décembre 2007, le consortium universitaire belge "Be Voting" énumère diverses solutions envisageables. La plupart d'entre elles combinent le recours à un équipement de vote électronique avec l'émission d'une trace papier explicite pour l'électeur. [Consortium de professeurs de KUL, UA, UG, UCL, ULg, ULB, VUB, 2007]

1.3 Vote par Internet ou I-vote

Avec l'arrivée et l'expansion d'Internet, le vote électronique par Internet a effectivement fait son entrée récemment dans les systèmes de vote utilisés. Le vote par Internet peut être

- soit local (l'électeur vient émettre son vote dans un isoloir et l'émission de son vote est automatiquement enregistrée sur un serveur connecté à Internet)
- soit global (l'électeur doit se connecter à Internet pour émettre son vote mais il peut se connecter à partir de chez lui, d'un espace public numérique ou de n'importe quel point d'accès à Internet).

De manière générale, nous parlerons de vote à distance (cette notion pouvant également être utilisée pour le vote par correspondance sur support papier) ou d'I-vote lorsque le recours à Internet est de mise. Dans le cas particulier où le vote a lieu dans un isoloir ou un lieu « protégé », il s'agit du vote en kiosque.

Pour illustrer ce concept d'I-vote, deux exemples récents d'élections par Internet sont évoqués ci-après.

1.3.1 L'Estonie, un exemple du vote par Internet !

L'OSCE / ODIHR (Organization for Security and Co-operation in Europe - Office for Democratic Institutions and Human Rights) a réalisé une mission d'observations lors des élections parlementaires en Estonie en mars 2007. C'était la première fois que le vote par Internet était disponible pour tous les électeurs lors d'élections législatives dans un pays membre de l'OSCE.

Le vote par Internet était disponible durant quelques jours (4 à 6 jours) avant le jour traditionnel des élections. L'électeur pouvait voter plusieurs fois durant cette période :

- soit un nouveau vote par Internet qui annulait ses votes précédents
- soit un vote papier émis dans un bureau de vote

La loi estonienne prévoit que le vote papier est prépondérant sur le vote par Internet. Il est donc prévu de supprimer tous les votes venant par Internet pour lesquels l'électeur est également passé dans le bureau de vote. Pour ce faire, il faut une connexion Internet dans chaque bureau de vote pour "marquer" ces électeurs dans le registre comme ayant voté via bulletin papier, et ainsi invalider leur I-vote.

Tout comme pour le vote par correspondance, un système à double enveloppe garantit l'anonymat du votant : le contenu du vote électronique n'est décrypté qu'après avoir été séparé de l'identité du votant après la période "avancée" du vote. Tout le processus de vote est rendu possible grâce à une carte ID électronique.

[*Office for Democratic Institutions and Human Rights, 2007*]

Cette possibilité de vote par Internet (méthode supplémentaire et non obligatoire) avait été introduite préalablement en 2005 lors des élections municipales. Elle avait créé de nombreuses controverses politiques et suscité beaucoup d'intérêt. Certes, elle augmente l'accès des électeurs au processus de vote, mais elle pose également de nombreux risques sur l'intégrité des élections à cause des possibilités de piratage ou d'erreurs de programmation. Ce point sera abordé au chapitre 3.

1.3.2 L'élection du recteur de l'Université Catholique de Louvain (UCL)

En mars 2009, les membres de l'UCL (professeurs, membres du personnel et étudiants) ont élu leur nouveau recteur, Bruno Delvaux, par I-vote. Cette élection s'est en effet déroulée via Internet, grâce à une solution technique conçue par le professeur Ben Adida (Harvard), le système HELIOS. L'avantage de ce système repose sur 3 points essentiels :

1. L'électeur peut contrôler chaque étape de l'élection
2. Le système garantit la confidentialité
3. Un vote erroné est pratiquement impossible

Ce système est appelé "open-audit" car l'audit complet de l'ensemble du processus est possible par tout observateur. Tout électeur peut en effet vérifier que chaque étape du processus de vote s'est passée correctement et que les résultats du vote sont corrects :

- Vérification que le bulletin électronique transmis correspond à l'intention de vote de l'électeur
- Vérification que ce bulletin est correctement comptabilisé lors du dépouillement

[Ben Adida, 2009]

Cette élection sera détaillée dans les prochains chapitres.

2 Procédure de vote corporatiste par Internet

Dans ce chapitre, nous allons observer et détailler différentes élections ou émissions de vote, dans le domaine corporatiste. Les cas étudiés correspondent à des organisations qui ont fait le choix (ou qui devront le faire prochainement) d'utiliser Internet pour l'émission de leur vote.
L'utilisation de l'informatique pour les élections (e-vote ou I-vote) est certes une évolution technologique mais remet également en question la légitimité des processus électoraux. Cette question pouvant devenir centrale, et vu le temps limité consacrée à l'étude, il fut décidé de s'attacher uniquement à des processus électoraux dits corporatistes. Dans ce domaine corporatiste, nous avons estimé qu'une plus large part d'arbitraire pouvait être tolérée.

2.1 Présentation de cas concrets

2.1.1 Les élections sociales en Belgique

Les élections sociales ont lieu tous les 4 ans en Belgique. Ces élections ont pour but de désigner les représentants des travailleurs pour les conseils d'entreprise et les comités pour la prévention et la protection au travail.

Toutes les sociétés ne doivent pas avoir ces organes :

- un conseil d'entreprise est obligatoire pour une entreprise employant au moins 100 personnes
- un comité pour la prévention et la protection au travail est obligatoire pour une entreprise employant au moins 50 personnes

Il s'agit spécifiquement des sociétés du secteur privé ayant une finalité économique et commerciale ainsi que les entreprises sans but lucratif comme les services sociaux et de santé.

Ces organes sont constitués en partie par les représentants de la direction de l'entreprise et en partie par les représentants des travailleurs, présentés par les syndicats et élus par les travailleurs.

Ces élections doivent respecter certaines conditions spécifiées dans un arrêté royal et reprises et explicitées dans une brochure éditée par le SPF Emploi, Travail et Concertation sociale. [Service public fédéral Emploi, Travail et concertation sociale, 2008]

Ces élections sont organisées par secteur d'activité. Le cas étudié se rapporte au domaine bancaire. La Febelfin (fédération du secteur financier belge) organise ces élections pour les banques.

Actuellement, ces élections se déroulent toujours principalement avec un vote papier, voire parfois via e-voting.

La campagne électorale de ces élections se fait exclusivement via support papier traditionnel.

Une convocation papier est envoyée aux électeurs par courrier (soit courrier interne sur leur lieu de travail soit courrier postal à leur domicile).

Il existe plusieurs catégories d'électeurs, chaque catégorie ayant ses propres candidats. En d'autres termes, chaque catégorie d'électeurs correspond à une circonscription électorale spécifique. Nous distinguons :

- jeunes travailleurs (travailleurs n'ayant pas atteint l'âge de 25 ans le jour de l'élection)
- employés ou ouvriers (en fonction de la déclaration ONSS)
- cadres

L'ensemble de la procédure électorale est détaillée dans un calendrier strict s'étalant sur 150 jours (voir détails en annexe 2)

Le vote se déroule de la façon suivante

- il y a réquisition d'assesseurs complémentaires si nécessaire
- l'électeur reçoit son bulletin de vote sur présentation de sa convocation et de sa carte d'identité (plusieurs listes sont proposées sur le bulletin)
- le panachage au niveau du vote est interdit
- l'électeur dépose son bulletin dans l'urne

A la fin du dépouillement, un procès verbal est rédigé et les résultats du vote sont envoyés. Cela permet la répartition des mandats. Les résultats sont alors communiqués officiellement et analysés.

Les directions des grandes banques belges sont désireuses de passer à l'i-voting. Des réflexions sont en cours pour les prochaines élections prévues en 2012. Des contacts ont été pris avec la Fédération des Entreprises de Belgique (FEB) mais vu les circonstances économiques actuelles, la gestion de la crise prime sur tout le reste.
Les points importants qui poussent les directions des banques à s'orienter vers cette évolution sont :

- gain de temps
- gain de productivité
- rapidité du dépouillement

Les syndicats ne sont pas opposés à l'idée mais veulent obtenir certaines garanties. Pour eux, le secret du vote est primordial ! Nous reviendrons sur cette notion dans le chapitre 3.

Actuellement, l'arrêté royal régissant les règles des élections sociales, propose et accepte uniquement l'usage du vote électronique (rien n'est encore prévu pour l'i-voting) selon le respect de certaines conditions :

- le système informatique doit être conforme à certaines dispositions propres à ce type d'élection
- des informations pour la rédaction du procès verbal doivent être enregistrées
- le système doit présenter un écran général avec toutes les listes ; puis, après sélection de l'électeur, présenter les candidats de la liste sélectionnée
- le système ne peut permettre l'enregistrement d'un vote nul
- le système doit être fiable et garantir la sécurité (empêcher la modification des données et garantir le secret du vote)

[D.C., 15/07/2009]

2.1.2 Les votes aux assemblées générales de sociétés cotées

Chaque société cotée en bourse doit tenir une assemblée générale de ses actionnaires chaque année. Lors de ces assemblées, des questions sont soumises au vote des actionnaires. Ces questions ou propositions peuvent être soumises soit par le Conseil d'Administration soit par un groupe d'actionnaires représentant au moins 20% du capital.

Selon un calendrier bien spécifique, la société cotée doit prévenir ses actionnaires de la tenue de la prochaine assemblée générale. Cette information se fait généralement par les médias. Les actionnaires doivent alors déposer leurs actions et les bloquer durant une certaine période avant l'assemblée générale et jusqu'au terme de celle-ci. Ils reçoivent alors une invitation qui leur permet d'y assister.

Lors de l'assemblée générale, seuls les actionnaires présents dans la salle peuvent prendre part aux votes (exception faite pour le vote par procuration). Cela signifie que, bien que l'assemblée générale soit diffusée en direct sur Internet, l'actionnaire internaute ne peut pas voter par Internet. Il doit être absolument présent physiquement dans la salle ou avoir donné procuration à un mandataire.
Cela pose certains problèmes pour les grands groupes ayant leur actionnariat dispersé à travers le monde. Dans cette optique, la Commission Européenne a pris une directive pour pousser les sociétés cotées à trouver une solution et un projet de loi en ce sens a été déposé fin juin 2009 en Belgique.
[CBFA, 2009]

La voix d'un actionnaire compte pour autant d'actions qu'il a déposées. Dans la société étudiée, l'actionnaire reçoit, en échange de son invitation, une carte magnétique reprenant le nombre de voix dont il dispose. Son vote sera donc multiplié par autant de voix mentionnées sur cette carte magnétique.

Lors de la phase des votes, le Président lit une proposition de vote et demande aux actionnaires de voter via leur boîtier électronique. Il s'agit donc d'un vote électronique.

Cependant, il ne s'agit pas d'un vote de listes comme nous le connaissons pour les élections sociales évoquées ci-dessus. Il s'agit ici plutôt d'un vote référendaire pour émettre son opinion (« pour », « contre », « abstention ») par rapport à la question posée par le Président.

Après chaque vote, les résultats sont affichés (« pour », « contre », « abstention ») en termes de pourcentages et de nombre de voix.

Le vote aux AG de sociétés cotées ne doit être secret que pour les questions ayant trait aux personnes (nomination ou révocation). En pratique, on constate que le vote est secret au moment de l'élection mais il est possible de relier l'électeur à son vote.

Cette faculté est parfois utilisé par certains mandataires, pouvant représenter plusieurs actionnaires importants, afin d'avoir la preuve qu'ils ont correctement émis la volonté des actionnaires qu'ils représentent.
Néanmoins, en aucun cas, il n'est possible pour un actionnaire de connaître le choix effectué par un autre actionnaire.

Dans d'autres banques, jusqu'en 2006, le vote se faisait encore à main levée. Les systèmes changent donc d'une société à une autre.
[A.G., 27/7/2009] [L.G., 10/8/2009]

2.1.3 L'élection du recteur de l'Université Catholique de Louvain

Comme déjà sommairement présenté dans le chapitre 1.3.2. L'élection du recteur de l'Université Catholique de Louvain (UCL), l'élection du recteur de l'UCL a été réalisé en 2009 par I-vote. Cette élection s'est en effet déroulée via Internet, grâce à une solution technique conçue par le professeur Ben Adida (Harvard), le système HELIOS. L'avantage de ce système repose sur 3 points essentiels :

1. L'électeur peut contrôler chaque étape de l'élection
2. Le système garantit la confidentialité
3. Un vote erroné est pratiquement impossible

Ce système est appelé "open-audit" car l'audit complet de l'ensemble du processus est possible par tout observateur. Tout électeur peut en effet vérifier que chaque étape du processus de vote s'est passée correctement et que les résultats du vote sont corrects :

- Vérification que le bulletin électronique transmis correspond à l'intention de vote de l'électeur
- Vérification que ce bulletin est correctement comptabilisé lors du dépouillement

Cette élection avait la particularité de présenter un scrutin pondéré (une voix d'un étudiant a moins de poids qu'une voix d'un membre du personnel académique).

Comme pour la plupart des élections, un calendrier spécifique est établi. Les moments-clés principaux sont

- Publication de la liste pré-électorale (via intranet)
- Publication de la liste des candidats
- Inscription sur les listes électorales (via Internet)
- 1er tour de scrutin (durant 2 jours)

Chaque électeur reçoit sa convocation par mail.

Puisqu'un nouvel outil était proposé pour cette élection, un scrutin-test était proposé pour se familiariser avec ce nouvel outil.

L'information relative à l'élection est publiée sur l'intranet ou via le journal d'entreprise électronique (« La Quinzaine »).

L'émission du vote se passe donc par Internet selon la procédure suivante

- le code d'accès devait être téléchargé à l'avance sur le site de l'élection, après identification de l'électeur
- l'électeur se connecte au site de l'élection
- l'électeur accède à son bulletin et vote (choix d'un candidat ou vote blanc)
- après confirmation du vote, celui-ci est chiffré et scellé

- l'électeur reçoit un numéro de suivi qui lui permettra de vérifier que son choix est bien pris en compte
- le numéro d'électeur et le code d'accès sont introduits pour l'envoi du vote

Après la phase de vote, il est possible pour l'électeur de vérifier sur les valves Internet que tout s'est bien passé. En cas de doute, la possibilité de re-voter est offerte (avec annulation du vote précédent).

Un candidat qui obtient plus de 50% des voix est élu ; sinon il y a un 2^{e} tour de scrutin

Pour garantir la disponibilité du système de vote, il fut décidé de faire appel à des serveurs externes puissants (Amazon et Google).
[Pierre Escayez, 1/12/2008]
[O.P., 2009] [J.J.Q., 2009]

2.1.4 Institute of Electrical and Electronics Engineers (IEEE)

L'Institute of Electrical and Electronics Engineers (IEEE) est une organisation ayant pour but de promouvoir la connaissance dans le domaine de l'ingénierie électrique. Elle regroupe des professionnels du domaine des télécommunications, de l'informatique, ...
L'IEEE publie ses propres normes ou des articles écrits par ses membres.

Des élections sont organisées pour chacun de ses organes, à travers le monde.
Il est logique que cette organisation voulant promouvoir les nouvelles technologies utilise l'I-voting pour ses élections. Néanmoins, les solutions d'I-voting sont fournies par des sociétés extérieures telles que

- « Survey & Ballot Systems (SBS) » pour l'élection annuelle et l'élection des organes "Circuit & Systems Society" et "Computer Society"
- Intelliscan pour d'autres organes
- ...

Des règles spécifiques et précises stipulent dans quelles conditions doivent se dérouler ces élections. Toutes ces règles sont expliquées en détail dans les « IEEE Policy et Bylaws » qui servent donc de référentiels pour ces élections. Les statuts (« Bylaws ») reprennent les détails pour les candidatures et le calendrier des élections

Pour l'organe principal de l'IEEE, il existe différentes élections

- Président du conseil d'administration de l'IEEE
- Directeur Régional : le monde est divisé en 10 régions IEEE, chacune représentée au conseil d'administration de l'IEEE par un Directeur Régional élu pour 2 ans
- Directeur de Division : l'IEEE est composée de 10 divisions techniques, chacune représentée au conseil d'administration de l'IEEE par un Directeur de Division élu pour 2 ans
- ...

Le conseil d'administration soumet chaque année une liste de candidats aux membres ayant le droit de vote.
Il est également possible de proposer une candidature via une pétition regroupant au minimum 600 signatures. Dans ce cas,

- l'IEEE vérifie les conditions d'éligibilité du candidat
- un calendrier spécifique doit être respecté pour introduire la pétition reprenant les signatures nécessaires
- la pétition doit reprendre certaines mentions spécifiques

La politique de l'IEEE prévoit d'informer tous les membres de la candidature et du point de vue de tous les candidats, y compris ceux par pétition et favorise l'échange d'idées.
Une campagne électorale payante dans les publications de l'IEEE n'est pas permise.

Par contre, chaque candidat réalise une déclaration selon des formes et une taille bien déterminées. Chaque candidat doit également fournir

- une photo
- un résumé de ses services au sein de l'IEEE
- une biographie personnelle, de son expérience hors de l'IEEE

Un site Internet est dédié chaque année aux élections, reprenant les informations concernant les candidats (l'existence de ce site web est annoncée via mail).

La procédure de vote par Internet (100% online) se déroule de la façon suivante

- chaque membre ayant droit de voter reçoit un mail avec un lien pour se connecter au site des élections
- l'identifiant et le mot de passe de son compte Web IEEE lui permettent de s'identifier et ensuite de signer son vote.

Pour les membres de l'IEEE, le vote reste secret puisque seule la société s'occupant de l'élection à accès aux informations détaillées ; l'IEEE ne reçoit que les résultats finaux.

Les résultats sont publiés et consultables en ligne.

Il existe également la possibilité de vote par correspondance papier :

- l'électeur qui a reçu un bulletin via la poste, le complète et le renvoie à la société qui fournit le service pour l'élection
- la partie du dessus identifiant l'électeur est détachée ; la partie du bas est comptabilisée (il y a ainsi une séparation entre les données de vote et les données identifiant l'électeur)

[C.L., 2009]
[IEEE Policies, 2008] [IEEE Bylaws, 2008]

2.2 Analyse, observations et comparaisons de ces élections

2.2.1 Présentation de l'article de référence

L'article publié dans la revue de l'IEEE « *E-election in Digital Society* » au moment de la « *2009 Third International Conference on Digital Society* » propose le cheminement complet de l'analyse d'une élection corporatiste.
[Mohamad Taghi Isaai, Fatemeh Firoozi, Mahmood Reza Hemyari, 2009]

Selon l'article, le développement d'une société numérique et électronique devient un défi majeur pour les pays développés. Cela provoque des révisions des processus et structures des organismes voulant intégrer cette société numérique. L'article précité se concentre principalement sur la partie de la société numérique consacrée aux élections électroniques.

Les auteurs tentent de définir les pré-requis nécessaires pour définir les étapes à franchir pour passer d'une élection traditionnelle à une élection purement électronique.

L'e-election telle que mentionnée dans cet article reprend les notions à la fois de vote électronique, mais également de vote en kiosque, de vote à distance et de vote par Internet. Dans le cadre de ce travail, ce terme d'e-election évoquera principalement le cas du vote par Internet.

L'article se consacre à l'étude du cas des élections de la « Teheran Trade Organization (TTO) » et au standard fixé par l' « Organization for the Advancement of Structured Information Standards (OASIS) ».

Les éléments importants de cet article sont détaillés ci-dessous (méthodologie de recherche, grille d'analyse, conditions d'acceptation, catégorisation).

2.2.1.1 Méthodologie de recherche employée

Une enquête fut menée par mails et par interviews auprès des futurs candidats et des membres de l'équipe de direction. Il y eut une analyse des réponses ainsi qu'une reconnaissance et une documentation du workflow de l'élection traditionnelle. Afin de normaliser le processus électoral, tous les standards communs (connus de OASIS) ont été consultés et Election Markup Language (EML) fut sélectionné pour devenir le cadre de référence. C'est ainsi que le processus électoral traditionnel restructuré par le cadre de référence EML fut proposé.

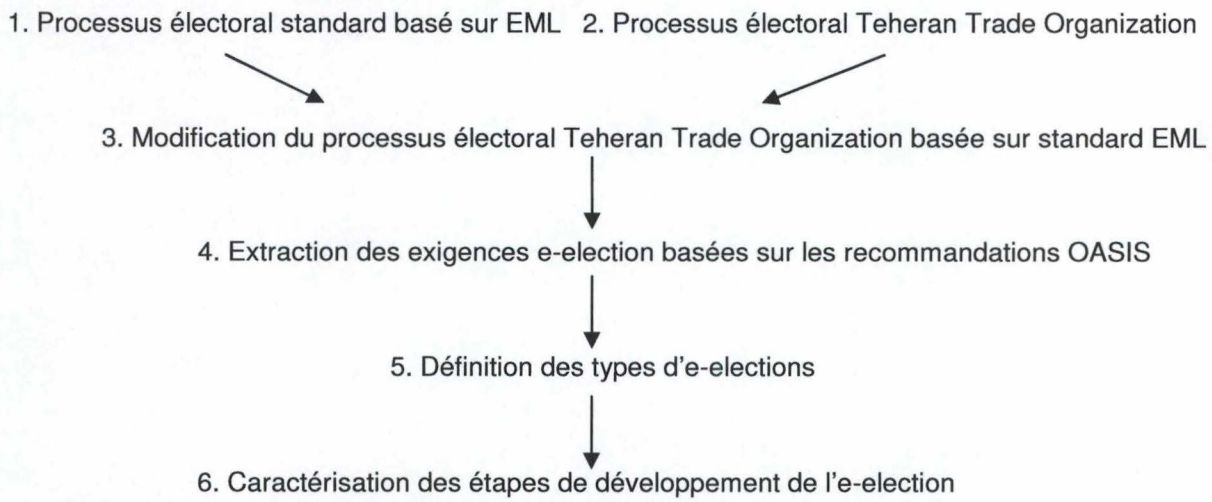


Figure 1: Etapes de recherche

Les 6 étapes reprises dans la figure ci-dessus ont été analysées par les auteurs de cet article dans le cadre de l'élection de la TTO afin de planifier l'implémentation du système d'I-voting pour cette élection.

2.2.1.2 Grille d'analyse selon 3 zones majeures

Selon OASIS, l'ensemble du processus de l'élection peut être divisé en 3 zones ou périodes majeures, chacune sous-divisée en processus d'élection ; les principaux étant :

- pré-élection
    - présentation de l'élection
    - candidat
        - inscription
        - réponse à la proposition d'inscription
        - liste de candidats
    - électeurs
        - inscription sur les listes électorales
        - liste électorale
        - communication aux électeurs
        - sondages / informations aux bureaux de vote
- élection
    - vote
        - bulletin de vote
        - authentification
        - réponse d'authentification
        - confirmation du vote
        - collectes de l'ensemble des votes
- post-élection
    - décompte
        - comptage des résultats
    - audit
    - analyse

2.2.1.3 Conditions d'acceptation – objectifs de sécurité

Pour être acceptés par les utilisateurs, les systèmes d'élection par Internet doivent garantir les propriétés de base d'un système électoral traditionnel tels que

- authentification
- transparence
- anonymat de l'électeur
- confidentialité & vie privée
- intégrité
- secret du vote

mais également des avantages supplémentaires tels que :

- **indépendance de localisation** (possibilité de voter à partir de n'importe quel endroit grâce à l'accès à Internet ; protocole basé sur une Public Key Infrastructure (PKI) pour garantir la confidentialité et le secret du vote)
- **système de sécurité** contre les attaques
- ...

2.2.1.4 Catégorisation du type d'élection

Pour catégoriser le type d'élection, cet article se base sur 3 axes :

- l'usage de périphériques orientés I-voting (device)
- la fréquentation / la participation sur Internet (attendance)
- l'automatisation des processus électoraux (process)

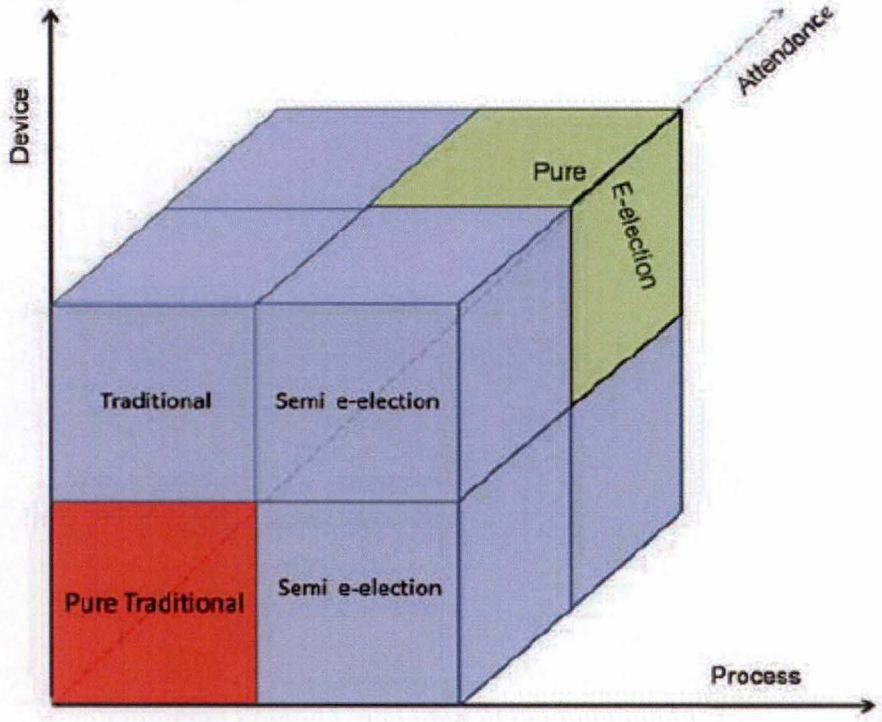


Figure 2: Catégorisation (schéma) du type d'élection selon 3 axes (automatisation des processus, participation sur Internet, périphériques orientés I-voting)

[Mohamad Taghi Isaai, Fatemeh Firoozi, Mahmood Reza Hemyari, 2009]

Le taux de participation sur Internet par rapport à la participation à l'élection via les services traditionnels devient un Key Performance Indicator (KPI) qui montre le succès et l'attractivité du système I-voting.

Cette catégorisation nous permet de présenter les différentes étapes du passage de l'élection traditionnelle pure à l'élection 100% online.

Election	Automatisation des processus	Participation sur Internet	Périphérique orienté i-voting	Description
Traditionnelle pure	0	0	0	Il n'existe aucune automatisation i-voting Aucune possibilité de signature digitale Aucun kiosque ou terminal pour i-voting
Semi-électronique	1	0	0	Certains / Tous les processus i-voting sont automatisés Aucune possibilité de signature digitale Aucun kiosque ou terminal pour i-voting
Traditionnelle	0	1	0	Il n'existe aucune automatisation i-voting La signature digitale rend possible le vote de n'importe où Aucun kiosque ou terminal pour i-voting
Traditionnelle	0	0	1	Il n'existe aucune automatisation i-voting Aucune possibilité de signature digitale Les terminaux pour i-voting et kiosques sont utilisés
Semi-électronique	1	1	0	Certains / Tous les processus i-voting sont automatisés La signature digitale rend possible le vote de n'importe où Aucun kiosque ou terminal pour i-voting
Semi-électronique	1	0	1	Certains / Tous les processus i-voting sont automatisés Aucune possibilité de signature digitale Les terminaux pour i-voting et kiosques sont utilisés
Traditionnelle	0	1	1	Il n'existe aucune automatisation i-voting La signature digitale rend possible le vote de n'importe où Les terminaux pour i-voting et kiosques sont utilisés
Pure électronique	1	1	1	Tous les processus i-voting sont automatisés La signature digitale rend possible le vote de n'importe où Les terminaux pour i-voting et kiosques sont utilisés

Figure 3: Catégorisation (tableau) du type d'élection selon 3 axes (automatisation des processus, participation sur Internet, périphériques orientés i-voting)

2.2.1.5 Chemins de développement

Cet article propose, pour terminer, un chemin de développement générique en 4 étapes :

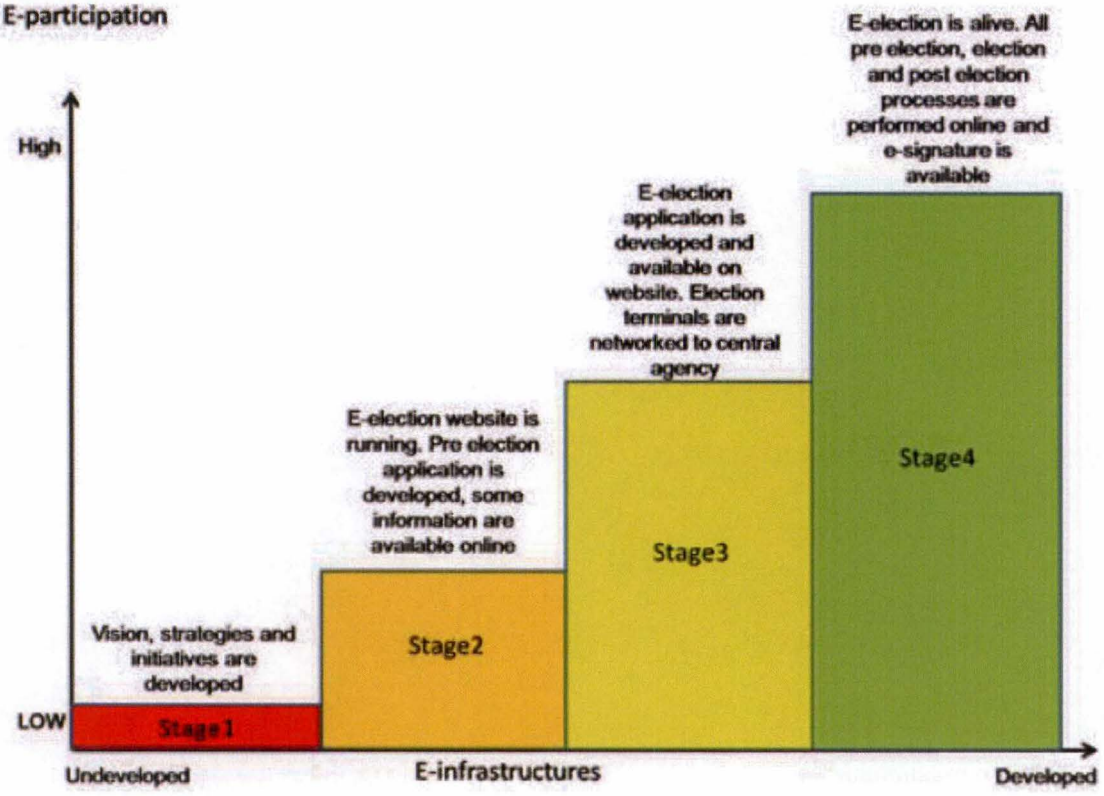


Figure 4: Chemin de développement

[Mohamad Taghi Isaai, Fatemeh Firoozi, Mahmood Reza Hemyari, 2009]

1. Situation « As-Is »
    a. Aucun formulaire électronique
    b. Enregistrement des candidatures sur papier
    c. Aucun site Internet pour fournir de l'information
    d. 3 processus principaux gérés manuellement
    e. Lois et réglementations I-voting peuvent exister ou être développées

2. Accès online aux informations de l'élection
    a. Page web ou site web officiel
    b. Enregistrement des candidatures complètement online
    c. Application « pré-élection » développée
    d. La plupart de l'information reste statique avec peu d'options pour l'utilisateur

3. Présence de l'élection online
    a. Application « élection » développée
    b. Tous les processus de l'élection sont en ligne
    c. Manque de la signature électronique → vote possible uniquement sur des terminaux de vote (kiosques, bureaux de vote, …)
    d. Bureaux de vote mis en réseau

4. L'I-voting existe
    a. Buts de l'élection sont réalisés
    b. Présentations des résultats personnalisables par l'utilisateur
    c. La signature électronique (basée sur PKI) existe et l'authentification a lieu online
    d. Portail de l'élection avec toutes les applications de l'élection
    e. La participation sur Internet (KPI) augmente au maximum

Ainsi, l'article conclut notamment avec l'offre grandissante des services online via Internet, principalement orientés business tels que e-commerce ou e-banking. Cependant, la participation sur Internet devient plus commune via les forums et les systèmes de vote. Au-dessus de tous les défis techniques, l'engagement de l'utilisateur et sa confiance dans le système demandent des recherches approfondies.

2.2.2 Grille d'analyse

Sur base de cet article, différents points (mentionnés ci-dessous) sont à reprendre dans la grille d'analyse, qui permettra l'analyse des différents systèmes électoraux.

- Zones majeures et sous-processus

Zone majeure	Sous-processus	Description Commentaire
Pré-élection	Présentation de l'élection	
	Candidat – inscription	
	Candidat – réponse à la proposition d'inscription	
	Candidat – liste de candidats	
	Electeurs – inscription sur les listes électorales	
	Electeurs – liste électorale	
	Electeurs – communication aux électeurs	
	Electeurs - sondages / informations aux bureaux de vote	
Election	Vote – bulletin de vote	
	Vote – authentification	
	Vote – réponse d'authentification	
	Vote – confirmation du vote	
	Vote – collectes de l'ensemble des votes	
Post-élection	Décompte – comptage des résultats	
	Audit	
	Analyse	

- Catégorisation du type d'élection (3 axes)

Ceci correspond à la grille proposée dans le chapitre 2.2.1.4. Catégorisation du type d'élection

- Etapes dans le chemin de développement

Ces étapes correspondent aux 4 étapes proposées dans le chapitre 2.2.1.5. Chemins de développement

2.2.3 Comparaison des cas étudiés, selon la grille d'analyse

2.2.3.1 Elections sociales en Belgique

Zones majeures et sous-processus

Zone majeure	Sous-processus	Description - Commentaire
Pré-élection	Présentation de l'élection	Campagne électorale papier
	Candidat – inscription	Procédure manuelle
	Candidat – réponse à la proposition d'inscription	Procédure manuelle
	Candidat – liste de candidats	Liste diffusée sous format papier
	Electeurs – inscription sur les listes électorales	Electeurs repris automatiquement sur base du registre du personnel
	Electeurs – liste électorale	Liste publiée sous format papier
	Electeurs – communication aux électeurs	Information transmise par courrier
	Electeurs - sondages / informations aux bureaux de vote	
Election	Vote – bulletin de vote	Bulletin papier
	Vote – authentification	Carte identité et convocation papier présentées au bureau de vote
	Vote – réponse d'authentification	Remise d'un bulletin de vote
	Vote – confirmation du vote	Cachet sur la convocation
	Vote – collecte de l'ensemble des votes	Urne traditionnelle
Post-élection	Décompte – comptage des résultats	Décompte manuel
	Audit	
	Analyse	Publication des résultats et brève analyse

Catégorisation du type d'élection

Election	Automatisation des processus	Participation sur Internet	Périphérique orienté i-voting	Description
Traditionnelle pure	0	0	0	Il n'existe aucune automatisation i-voting Aucune possibilité de signature digitale Aucun kiosque ou terminal pour i-voting

Etapes dans le chemin de développement

Etape 1 : Situation « As-Is »

a. Aucun formulaire électronique
b. Enregistrement des candidatures sur papier
c. Aucun site Internet pour fournir de l'information
d. 3 processus principaux gérés manuellement
e. Lois et réglementations I-voting peuvent exister ou être développées

2.2.3.2 Votes lors d'une assemblée générale d'une société cotée

Zones majeures et sous-processus

Zone majeure	Sous-processus	Description - Commentaire
Pré-élection	Présentation de l'élection	Publication de l'avis de la future AG dans la presse spécialisée, sur le site Internet de la société
	Candidat – inscription	Pas d'inscription de candidat Questions/Propositions soumises au vote, introduites par le Conseil d'Administration ou par un groupe d'actionnaires représentant au moins 20% du capital (procédure manuelle)
	Candidat – réponse à la proposition d'inscription	Procédure manuelle
	Candidat – liste de candidats	Questions/Propositions reprises dans le document accompagnant l'invitation
	Electeurs – inscription sur les listes électorales	Dépôt des actions de l'actionnaire durant la période de l'AG
	Electeurs – liste électorale	Liste électorale non publiée (respect de la vie privée) mais disponible au siège de la société via les listes des actions déposées
	Electeurs – communication aux électeurs	Presse spécialisée ou site Internet
	Electeurs - sondages / informations aux bureaux de vote	
Election	Vote – bulletin de vote	Boîtier électronique
	Vote – authentification	Carte à puce remise à l'accueil après vérification de la carte d'identité, de l'invitation et du nombre de voix
	Vote – réponse d'authentification	
	Vote – confirmation du vote	Boîtier électronique
	Vote – collecte de l'ensemble des votes	Urne électronique
Post-élection	Décompte – comptage des résultats	Automatique et directement après chaque vote Affichage du résultat sous forme pourcentage et nombre (« pour », « contre », « abstentions »)
	Audit	Possibilité pour un électeur de demander la vérification de son vote (visiblement, d'application pour les mandataires de plusieurs actionnaires)
	Analyse	

Catégorisation du type d'élection

Election	Automatisation des processus	Participation sur Internet	Périphérique orienté i-voting	Description
Semi-électronique	1	0	1	Certains / Tous les processus i-voting sont automatisés Aucune possibilité de signature digitale Les terminaux pour i-voting et kiosques sont utilisés

Etapes dans le chemin de développement

Etape 2 : Accès online aux informations de l'élection

a. Page web ou site web officiel
b. Enregistrement des candidatures complètement online
c. Application « pré-élection » développée
d. La plupart de l'information reste statique avec peu d'options pour l'utilisateur

2.2.3.3 Election du recteur de l'Université Catholique de Louvain

Zones majeures et sous-processus

Zone majeure	Sous-processus	Description - Commentaire
Pré-élection	Présentation de l'élection	Information via le journal électronique (« La Quinzaine »)
	Candidat – inscription	Procédure manuelle
	Candidat – réponse à la proposition d'inscription	Procédure manuelle
	Candidat – liste de candidats	Publication sur intranet et via le journal électronique (« La Quinzaine »)
	Electeurs – inscription sur les listes électorales	Invitation par courrier électronique pour s'inscrire en ligne sur le site de l'élection
	Electeurs – liste électorale	Listes pré-électorale et électorale publiées sur intranet
	Electeurs – communication aux électeurs	Journal électronique (« La Quinzaine ») + convocation par email
	Electeurs - sondages / informations aux bureaux de vote	
Election	Vote – bulletin de vote	Disponible en ligne après authentification
	Vote – authentification	Via identifiant UCL + numéro carte membre personnel / étudiant
	Vote – réponse d'authentification	Accès au site de l'élection, partie sécurisée
	Vote – confirmation du vote	Réception d'un numéro de suivi qui permettra à l'électeur de vérifier que son vote a bien été pris en compte
	Vote – collecte de l'ensemble des votes	Affichage sur les valves Internet des votes chiffrés
Post-élection	Décompte – comptage des résultats	Traitement des données chiffrées et anonymes par des logiciels indépendants. Déchiffrement d'un seul message chiffré : le résultat pondéré de l'élection
	Audit	Audit possible à tout moment de la procédure par tout électeur Vérification possible à posteriori par toute personne en faisant la demande des logiciels et des données utilisés
	Analyse	

Catégorisation du type d'élection

Election	Automatisation des processus	Participation sur Internet	Périphérique orienté i-voting	Description
Semi-électronique	1	0	1	Certains / Tous les processus i-voting sont automatisés Aucune possibilité de signature digitale Les terminaux pour i-voting et kiosques sont utilisés
Pure électronique	1	1	1	Tous les processus i-voting sont automatisés La signature digitale rend possible le vote de n'importe où Les terminaux pour i-voting et kiosques sont utilisés

Etapes dans le chemin de développement

Etape 3 : Présence de l'élection online

a. Application « élection » développée
b. Tous les processus de l'élection sont en ligne
c. Manque de la signature électronique → vote possible uniquement sur des terminaux de vote (kiosques, bureaux de vote, ...)
d. Bureaux de vote mis en réseau

Etape 4 : L'i-voting existe

a. Buts de l'élection sont réalisés
b. Présentations des résultats personnalisables par l'utilisateur
c. La signature électronique (basée sur PKI) existe et l'authentification a lieu online
d. Portail de l'élection avec toutes les applications de l'élection
e. La participation sur Internet (KPI) augmente au maximum

2.2.3.4 Election annuelle de l'IEEE

Zones majeures et sous-processus

Zone majeure	Sous-processus	Description - Commentaire
Pré-élection	Présentation de l'élection	Campagne électorale automatisée et disponible en ligne
	Candidat – inscription	Online
	Candidat – réponse à la proposition d'inscription	Online – via mail
	Candidat – liste de candidats	Disponible en ligne
	Electeurs – inscription sur les listes électorales	Électeurs repris directement sur base de sa qualité de membre de l'organisation
	Electeurs – liste électorale	
	Electeurs – communication aux électeurs	Via mail ou via le site de l'organisation ou de l'élection
	Electeurs - sondages / informations aux bureaux de vote	
Election	Vote – bulletin de vote	Électronique
	Vote – authentification	Mot de passe + identifiant
	Vote – réponse d'authentification	Accès à l'unique bulletin de vote
	Vote – confirmation du vote	
	Vote – collecte de l'ensemble des votes	Urne électronique
Post-élection	Décompte – comptage des résultats	Tout se passe au sein de la société en charge de l'élection
	Audit	
	Analyse	

Catégorisation du type d'élection

Election	Automatisation des processus	Participation sur Internet	Périphérique orienté i-voting	Description
Pure électronique	1	1	1	Tous les processus i-voting sont automatisés La signature digitale rend possible le vote de n'importe où Les terminaux pour i-voting et kiosques sont utilisés

Etapes dans le chemin de développement

Etape 4 : L'i-voting existe

a. Buts de l'élection sont réalisés
b. Présentations des résultats personnalisables par l'utilisateur
c. La signature électronique (basée sur PKI) existe et l'authentification a lieu online
d. Portail de l'élection avec toutes les applications de l'élection
e. La participation sur Internet (KPI) augmente au maximum

En conclusion, l'étude de ces quatre systèmes illustre différentes étapes de progression d'une élection purement traditionnelle (100% papier) vers une élection 100% online.

3 Analyse de risques

Dans ce chapitre, les aspects de sécurité seront abordés plus en détails. Quels sont les objectifs de sécurité à atteindre pour satisfaire aux exigences d'un vote corporatiste par Internet ? Notre référence sera la norme ISO/IEC 13 335-1 qui nous propose 7 objectifs de sécurité.

Pour commencer, après une brève description de cette norme ISO, les exigences de sécurité du groupe d'opposants au vote automatisé PourEVA seront présentées.
Ensuite, un premier aspect de sécurité sera étudié : les périphériques orientés I-voting (un des 3 axes observés dans le chapitre précédent pour la catégorisation d'une élection).
Le point principal de ce chapitre sera l'analyse de risque basée sur les recommandations du Conseil de l'Europe (référentiel) pour les étapes de vote et de dépouillement.
Dans chaque cas, une synthèse des objectifs de sécurité abordés sera présentée.
Une opposition importante entre secret du vote et vérifiabilité du vote sera également abordée.
Enfin, nous terminerons avec une synthèse des 7 objectifs de sécurité de la norme ISO/IEC 13 335-1 rencontrés tout au long de ce chapitre.

3.1 Objectifs de sécurité : norme ISO/IEC 13 335-1.

L'IEC (International Electrotechnical Commission) est l'organisation internationale de normalisation chargée des domaines de l'électricité, de l'électronique et des techniques connexes. Elle est complémentaire à l'ISO (Organisation internationale de normalisation) qui est chargées des autres domaines.
[IEC, 2009]

La norme ISO/IEC 13335 - Directives pour la gestion de la sécurité des Technologies d'information (Guidelines for the management of IT Security) - porte sur des directives concrètes pour la sécurité IT. Elle est composée de 4 parties ; la plus connue étant la première, intitulée « Concepts et modèles pour la gestion de la sécurité des technologies de l'information et des communications ».
[guideinformatique.com, 2009]
[Agence Nationale de la Sécurité Informatique, 2006]

Cette norme se base donc sur 7 objectifs de sécurité :

- **Confidentialité** : seules les personnes en communication ont accès à l'information ; les autres personnes ne peuvent pas comprendre l'échange d'information.
- **Intégrité** : Propriété de préservation de l'exactitude et de la complétude d'un bien.
- **Authenticité** : Propriété qui assure que l'identité d'un sujet ou d'une ressource est bien celle déclarée. L'authenticité s'applique à des entités telles que utilisateurs, processus, systèmes et information.
- **Disponibilité** : Propriété d'être accessible et utilisable à la demande d'une entité autorisée.

- **Imputabilité** : Propriété qui assure que les actions d'une entité peuvent être tracées et imputées à cette entité, de manière univoque
- **Non répudiation** : Capacité de prouver qu'une action ou un événement s'est présenté, sans que cette action ou cet événement ne puisse être infirmé ultérieurement
- **Fiabilité** : Propriété d'un comportement ou de résultats conformes aux attentes

[Région Wallonne, 2009]

3.2 Des associations veillent à la sécurité du vote électronique

À côté des études faites pour la promotion du vote électronique et du vote par Internet en particulier, d'autres associations veillent à la sécurité du vote électronique.

3.2.1 Pour une Ethique du Vote Automatisé

PourEVA est une association indépendante de tout parti politique regroupant des citoyens contestant le vote automatisé tel qu'il est utilisé actuellement en Belgique.
Il semble qu'une grande partie des membres de cette association soit des informaticiens sensibles aux risques et aux dangers que les solutions actuelles proposent.

Cette association part du principe que, pour le vote automatisé, le contrôle des opérations démocratiques n'est plus dans les mains du citoyen mais uniquement dans les mains des techniciens des firmes qui ont installé le matériel informatique.
L'association dit ne pas être opposée aux technologies (ils acceptent, par exemple, le dépouillement par lecture optique) mais désire revenir à un système qui permette au citoyen de contrôler le déroulement du processus électoral. Selon eux, le secret du vote est également menacé ! [Pour une Ethique du Vote Automatisé (Vote Electronique)]

3.2.2 Objectif(s) de sécurité abordé(s)

Confidentialité	Le **secret du vote** est menacé
Imputabilité	Le contrôle des opérations démocratiques n'est plus dans les mains du citoyen ou de l'électeur (**contrôle citoyen**)

3.3 Risque local à la machine « client »

Comme mentionné dans le chapitre 2.2.1.4. Catégorisation du type d'élection, l'usage de périphériques orientés I-voting est un paramètre qui permet de catégoriser une élection.
Pour utiliser Internet, nous pouvons considérer plusieurs périphériques tels que

- un serveur
- un réseau
- une machine « client »

Cette machine « client » est en fait la machine sur laquelle l'utilisateur interagit avec le système. Dans le cas d'une élection, c'est sur cette machine que l'électeur se connectera pour émettre son vote.
Le fait d'utiliser cette machine dans un isoloir ou pas sera abordé spécifiquement dans le chapitre 3.5.3. Absence d'isoloir.

Dans ce chapitre, nous nous consacrerons donc à l'étude du 1er risque potentiel : le risque local à la machine « client ». En effet, il est inutile de prévoir de grands algorithmes performants si on ne peut garantir que l'émission du vote sur la machine « client » ne s'est pas déroulé correctement.

3.3.1 La Suisse, de nombreux référendums... la piste électronique est envisagée également !

La Suisse est un pays où de nombreux référendums et/ou élections sont régulièrement organisés.
Genève est une collectivité publique qui œuvre en faveur du vote électronique par Internet et qui organise régulièrement des scrutins officiels en ligne. Le projet du vote par Internet a débuté en 2000 avec un projet fédéral sur l'utilisation des technologies de l'information dans le cadre des institutions démocratiques.
On considère le vote à distance par Internet comme la combinaison du vote à distance et du vote électronique. Le vote par correspondance est accepté à Genève depuis 1995 ; le vote électronique se généralise en Europe via des machines à voter. [E-voting du Canton de Genève]

Néanmoins, à côté de cela, le professeur Rolf Oppliger tempère quelque peu les ardeurs.
Pour lui, un problème majeur se pose : comment garantir la sécurité des plates-formes « clients » à partir desquelles les votes sont émis ? Virus, cheval de Troie et autres logiciels malveillants menacent la sécurité du vote ! Les anti-virus n'apportent une solution que pour les virus connus.

Quelques pistes de solution pour garantir la sécurité des plates-formes « clients » :

- *la distribution, par l'Etat, d'un CD permettant de garantir un système d'exploitation et une application de vote « sains »*

Cette solution est théoriquement intéressante mais difficile à mettre en pratique et très coûteuse !

- *un dispositif spécial de sécurité pour les PC s'occuperait de tout ce qui a trait au vote ; ce dispositif étant connecté, par exemple à partir du port USB*

Cette solution s'avère coûteuse également et oblige l'Etat à distribuer ce dispositif.

- *des systèmes d'exploitation de PC sûrs*

Cela s'avère très difficile à mettre en œuvre.

- *des feuilles de codes ou « vote par chiffrement »*

Chaque électeur reçoit une feuille reprenant un code pour chaque choix possible. Il introduit le code correspondant à son choix et le serveur lui renvoie un code de vérification. Ce code de vérification doit également se trouver sur la feuille de codes initialement reçue. Si les codes correspondent, l'électeur peut confirmer son choix.
Cette solution est fortement recommandée par le rapport du professeur Oppliger.

- *des scrutins tests*

Cette solution seule, basée sur les statistiques, n'est pas suffisante.
[Dr Rolf Oppliger, 2002]

Dans ce type de situation, nous réalisons une analyse de risque dans laquelle les éléments suivants sont étudiés :

- faille
- menace
- impact potentiel
- vulnérabilité

Dans le cas présent, nous pouvons étudier ces différents éléments de manière générale.

Faille	Machine « client » non sécurisée (virus, logiciel malveillant, système d'exploitation non sûr, ...)
Menace	Manipulation du vote à l'insu de l'électeur
Impact potentiel	Impact important Certains virus mettent du temps avant d'être décelés et peuvent se propager à une vitesse fulgurante Certains systèmes d'exploitation ou browser Internet ont une place de marché importante et donc un nombre potentiels d'électeurs très élevé
Vulnérabilité	Risque moyen Sans mesure spécifique de la part de l'organisation de l'élection, il est impossible de garantir que les machines « client » sont saines Le comportement à risques de certains utilisateurs d'Internet augmente ce risque D'un autre côté, une manipulation à grande échelle à ce niveau passerait difficilement inaperçue à moins que tous les électeurs ne connaissent strictement rien à l'informatique

3.3.2 Objectif(s) de sécurité abordé(s)

Intégrité	Il est difficile de garantir la sécurité de la machine « client » (**intégrité de la machine « client »**)

3.4 Recommandations du Conseil de l'Europe pour les votes automatisés.

3.4.1 Présentation des recommandations du Conseil de l'Europe et analyse de risque

Le Conseil de l'Europe s'est penché sur la question des votes électroniques et des votes par Internet.
Une première constatation fut que de nombreux pays européens utilisent déjà ou envisagent d'utiliser le vote électronique à plusieurs fins, et notamment pour

- permettre aux électeurs d'enregistrer leur vote ailleurs que dans le bureau de vote de leur circonscription électorale
- faciliter l'enregistrement du vote
- faciliter la participation aux élections, surtout pour les citoyens à l'étranger
- étendre l'accès au scrutin aux personnes ayant des problèmes de mobilité et d'accessibilité
- accroître la participation aux scrutins
- adapter les élections à l'évolution de la société et à l'utilisation croissante des nouvelles technologies
- fournir plus rapidement des résultats fiables
- offrir plusieurs modes de suffrages

Néanmoins, il faut garantir

- la fiabilité et la sécurité du processus
- le respect des règles démocratiques en vigueur (suffrage universel, suffrage libre, vote secret, ...)
- le respect des procédures (transparence, vérification et responsabilité, ...)
- ...

Dans cette optique, le Conseil de l'Europe a donc proposé, en 2004, 112 recommandations en reprenant

- les normes juridiques (suffrage universel, suffrage libre, vote secret, ...)
- les normes opérationnelles (notification, électeurs, candidats, ...)
- les exigences techniques (accessibilité, interopérabilité, sécurité, audit, ...).

[Comité des Ministres du Conseil de l'Europe, 2004]

Le chapitre 2. Procédure de vote corporatiste par Internet montre que chaque type d'élection a ses propres spécificités. En effet, dans certains cas, par exemple, il faut s'inscrire comme électeur alors que, dans d'autres cas, la qualité de membre de l'association suffit à être repris comme électeur.

L'analyse de risque proposée dans ce chapitre se consacrera au point central de chaque élection : le vote et le stockage du vote. Ce processus se retrouve de manière +/- identique dans chaque élection. Il est dès lors intéressant de se focaliser sur ce point principalement.

Les recommandations du Conseil de l'Europe que tout système électronique devra respecter pour être accepté correspondent donc à la norme actuelle à respecter.

Enfin, nous constatons que ces recommandations correspondent au référentiel public le plus connu actuellement dans la matière. Pour les élections législatives en Estonie, ces recommandations n'ont pas été entièrement suivies. Dans le cadre des élections corporatistes qui servent de scénario de base à ce travail, nous utiliserons ces recommandations. Néanmoins, nous devons être conscients des limites créées par l'application de consignes génériques à un scénario plus spécifique. Faute de mieux (quel autre référentiel reprendre ?), nous nous résoudrons à accepter cette solution !

Toutes les recommandations ne seront pas abordées dans ce travail. Par exemple, toutes celles ayant trait à l'interface Homme-Machine ne seront pas spécifiquement abordées dans ce travail.

Ces recommandations sont détaillées en annexe. Une croix dans la dernière colonne signifie que cette recommandation relève d'un aspect « sécurité ». Seules les recommandations relevant d'un aspect « sécurité » et consacrées au vote ou au stockage du vote seront abordées dans cette analyse de risque.

Pour établir notre analyse de risque, nous nous sommes appuyés sur ces notions de menace, d'impact potentiel et de vulnérabilité. Les descriptions et estimations données sont donc le résultat de l'analyse de l'auteur et nullement une source officielle du Conseil de l'Europe.
Pour chaque recommandation, la faille correspond à la recommandation, proposée par le Conseil de l'Europe, qui ne serait pas suivie.

Suffrage équitable...

Recommandation 5

Dans toute élection ou référendum, un électeur ne pourra pas déposer plus d'un seul bulletin dans l'urne électronique. Un électeur ne sera autorisé à voter que s'il est établi que son bulletin n'a pas encore été déposé dans l'urne électronique.

Menace	Plusieurs bulletins par électeur
Impact potentiel	Impact important Nombre de votes supérieur au nombre d'électeurs
Vulnérabilité	Risque faible

Rec. 6

Le système de vote électronique empêchera l'électeur d'exprimer son vote par plusieurs modes de suffrage.

Menace	Plusieurs bulletins par électeur
Impact potentiel	Impact important Nombre de votes supérieur au nombre d'électeurs
Vulnérabilité	Risque faible

Rec. 7

Tout bulletin déposé dans une urne électronique sera comptabilisé, et tout suffrage exprimé lors d'une élection ou d'un référendum ne sera comptabilisé qu'une seule fois.

Menace	Plusieurs bulletins par électeur / Aucun bulletin par électeur
Impact potentiel	Impact important Nombre de votes différent (inférieur ou supérieur) au nombre d'électeurs
Vulnérabilité	Risque faible

Rec. 8

Lorsque des modes de votes électroniques et non électroniques sont utilisés dans un même scrutin, une méthode sûre et fiable permettra d'additionner tous les suffrages et de calculer le résultat correct.

Menace	Addition incorrecte des voix
Impact potentiel	Impact important Nombre de votes différent (inférieur ou supérieur) au nombre d'électeurs
Vulnérabilité	Risque faible

Suffrage libre...

Rec. 9

L'organisation du vote électronique garantira la libre formation et expression de l'opinion de l'électeur et, au besoin, l'exercice personnel du droit de vote.

Menace	Perte du secret / confidentialité du vote
Impact potentiel	Impact réduit Manipulations, pressions
Vulnérabilité	Risque important Impossible de garantir la confidentialité sans isoloir

Rec. 11

Les électeurs pourront modifier leur choix à n'importe quelle étape de la procédure de vote électronique avant l'enregistrement de leur suffrage, ou même interrompre la procédure, sans que leur choix précédent ne soit enregistré ou que des tiers puissent en prendre connaissance

Menace	Impossibilité de corriger une erreur lors du choix de vote
Impact potentiel	Impact réduit Manipulations, pressions Erreurs
Vulnérabilité	Risque faible

Rec. 12

Le système de vote électronique n'autorisera pas les influences destinées à manipuler la volonté de l'électeur pendant le vote.

Menace	Perte du secret / confidentialité du vote
Impact potentiel	Impact réduit (niveau physique)
	Manipulations, pressions, ventes de vote
Vulnérabilité	Risque important
	Impossible de garantir la confidentialité sans isoloir

Rec. 15

Le système de vote électronique rendra impossible toute modification d'un suffrage une fois qu'il aura été enregistré.

Menace	Correction d'un vote après enregistrement
Impact potentiel	Impact important
	Modification du vote une fois déposé dans l'urne
Vulnérabilité	Risque faible

Vote secret...

Rec. 16

Le vote électronique sera organisé de manière à préserver le secret du vote à toutes les étapes de la procédure et en particulier lors de l'authentification de l'électeur.

Menace	Perte du secret du vote
Impact potentiel	Impact réduit au niveau physique
	Manipulations, pressions, ventes de vote
	Impact important au niveau logiciel
Vulnérabilité	Risque important au niveau physique
	Impossible de garantir la confidentialité sans isoloir
	Risque faible au niveau logiciel
	Mesures prises au niveau logiciel

Rec. 17

Le système de vote électronique garantira que les suffrages exprimés dans l'urne électronique et le dépouillement sont et resteront anonymes et qu'il est impossible d'établir un lien entre le vote et l'électeur.

Menace	Perte du secret / confidentialité du vote
Impact potentiel	Impact important (niveau logiciel)
	Manipulations, pressions, ventes de vote
Vulnérabilité	Risque faible
	Mesures prises au niveau logiciel

Rec. 18

Le système de vote électronique sera conçu de telle manière que le nombre de suffrages attendus dans une urne électronique ne permette pas d'établir un lien entre le résultat et les électeurs individuels.

Menace	Perte du secret du vote
Impact potentiel	Impact important
	Manipulations, pressions
Vulnérabilité	Risque faible
	Mesures prises au niveau logiciel

Rec. 19

Des mesures seront prises pour que les informations requises lors du traitement électronique ne puissent être utilisées pour violer le secret du vote

Menace	Perte du secret du vote
Impact potentiel	Impact important
	Manipulations, pressions
Vulnérabilité	Risque faible
	Mesures prises au niveau logiciel

Vérification et responsabilité...

Rec. 26

Le système offrira une possibilité de second dépouillement. D'autres caractéristiques du système de vote électronique qui pourraient peser sur l'exactitude du résultat seront vérifiables.

Menace	Erreur lors du dépouillement
Impact potentiel	Impact important
Vulnérabilité	Risque faible
	Les données peuvent être réutilisées pour un nouveau comptage

Fiabilité et sécurité...

Rec. 29

Toutes les mesures possibles seront prises pour écarter les risques de fraude ou d'intervention non autorisée affectant le système pendant toute la procédure du vote

Menace	Fraude
Impact potentiel	Impact important
Vulnérabilité	Risque faible
	Système informatique situé dans un endroit hautement sécurisé

Rec. 30

Le système de vote électronique comportera des mesures visant à préserver la disponibilité de ses services durant la procédure de vote électronique. Il résistera en particulier aux dérangements, aux pannes et aux attaques en déni de service

Menace	Panne, blocage, site inaccessible
Impact potentiel	Impact important
	Election peut être bloquée et de nombreux électeurs pourraient ne pas avoir accès au vote
Vulnérabilité	Risque moyen
	Utiliser des serveurs suffisamment puissants réduit le risque

Rec. 34

Le système de vote électronique préservera la disponibilité et l'intégrité des suffrages. Il assurera également leur confidentialité et les gardera scellés jusqu'au moment du dépouillement. Si les suffrages sont stockés ou transmis hors des environnements contrôlés, ils seront cryptés

Menace	Perte de suffrages, modification de suffrages
Impact potentiel	Impact très important
Vulnérabilité	Risque moyen
	Utiliser des serveurs suffisamment puissants réduit le risque
	Cryptographie et autres processus de sécurité à mettre en place

Rec. 35

Les votes et les informations relatives aux électeurs resteront scellés aussi longtemps que ces données seront conservées d'une manière qui permette d'établir le lien entre les deux. Les informations d'authentification seront séparées de la décision de l'électeur à une étape prédéfinie de l'élection électronique ou du référendum électronique

Menace	Perte du secret du vote
Impact potentiel	Impact important
	Manipulations, pressions
Vulnérabilité	Risque faible
	Mesures prises au niveau logiciel

Vote...

Rec. 44

Lorsque le vote électronique à distance se déroule pendant l'ouverture des bureaux de vote, il conviendra tout particulièrement de veiller à ce que le système soit conçu de manière à empêcher tout électeur de voter plusieurs fois

Menace	Plusieurs bulletins par électeur
Impact potentiel	Impact important
	Nombre de votes supérieur au nombre d'électeurs
Vulnérabilité	Risque faible

Rec. 51

Le système de vote électronique à distance ne permettra pas à l'électeur d'obtenir une preuve du contenu du suffrage qu'il a enregistré

Menace	Perte du secret du vote
Impact potentiel	Impact important
	Manipulations, pressions, ventes de votes
Vulnérabilité	Risque moyen
	Mesures prises au niveau logiciel (diminution du risque)
	Appareil photo ou copie d'écran (augmentation du risque)

Résultats...

Rec. 53

Le système de vote électronique ne permettra pas de divulguer le nombre de suffrages exprimés pour les différentes options de vote avant la fermeture de l'urne électronique. Cette information ne sera révélée au public qu'après la clôture de la période du scrutin

Menace	Perte de secret du vote si résultats partiels possibles
Impact potentiel	Impact moyen
	Il faudrait des résultats partiels fréquents pour pouvoir déterminer les identités des électeurs
Vulnérabilité	Risque faible
	Processus de dépouillement ne peut pas commencer avant la fin de l'élection

Rec. 54

Le système de vote électronique empêchera que le traitement d'informations relatives aux suffrages exprimés relativement à des sous-ensembles de votants choisis délibérément puisse révéler les décisions individuelles des électeurs

Menace	Perte de secret du vote si résultats partiels possibles
Impact potentiel	Impact moyen
	Il faudrait des résultats partiels fréquents pour pouvoir déterminer les identités des électeurs
Vulnérabilité	Risque faible
	Processus de dépouillement ne peut pas commencer avant la fin de l'élection

Rec. 55

Tout décodage nécessaire au dépouillement des voix interviendra dès que possible après la clôture de la période de scrutin

Menace	Perte d'informations (si traitement trop tardif)
	Perte de secret du vote si résultats partiels possibles (si traitement avant clôture du scrutin)
Impact potentiel	Impact moyen
	Il faudrait des résultats partiels fréquents pour pouvoir déterminer les identités des électeurs
Vulnérabilité	Risque faible
	Processus de dépouillement ne peut pas commencer avant la fin de l'élection

Fonctionnement des systèmes (pour l'infrastructure centrale et les clients dans des environnements contrôlés)...

Rec. 70

Les personnes en charge du fonctionnement des équipements définiront une procédure de secours. Tout système de remplacement répondra aux mêmes normes et exigences que le système original.

Menace	Panne, blocage, site inaccessible
Impact potentiel	Impact important
	Election peut être bloquée et de nombreux électeurs pourraient ne pas avoir accès au vote
Vulnérabilité	Risque moyen
	Utiliser des serveurs suffisamment puissants réduit le risque
	Duplication de l'information réduit le risque (back-up)

Rec. 71

Des mesures de secours suffisantes seront mises en place et disponibles en permanence afin d'assurer un déroulement sans heurt du scrutin. Le personnel concerné sera prêt à intervenir rapidement selon une procédure établie par les autorités électorales compétentes.

Menace	Panne, blocage, site inaccessible
Impact potentiel	Impact important
	Election peut être bloquée et de nombreux électeurs pourraient ne pas avoir accès au vote
Vulnérabilité	Risque moyen
	Utiliser des serveurs suffisamment puissants réduit le risque
	Duplication de l'information réduit le risque (back-up)

Rec. 72

Les responsables de l'équipement disposeront de procédures pour garantir que, durant le déroulement du scrutin, les équipements de vote et leur utilisation satisfont aux exigences requises. Des protocoles de contrôle seront régulièrement fournis aux services de secours

Menace	Panne, blocage, site inaccessible
Impact potentiel	Impact important Election peut être bloquée et de nombreux électeurs pourraient ne pas avoir accès au vote
Vulnérabilité	Risque moyen Utiliser des serveurs suffisamment puissants réduit le risque Duplication de l'information réduit le risque (back-up)

Rec. 74

Toute opération technique sera soumise à une procédure officielle de contrôle. Tout changement substantiel sur un équipement clé sera notifié.

Menace	Panne, blocage, site inaccessible Fraude en introduisant un équipement infecté d'un virus
Impact potentiel	Impact important Election peut être bloquée et de nombreux électeurs pourraient ne pas avoir accès au vote
Vulnérabilité	Risque faible Mesures à prendre

Rec. 75

Les équipements clés du vote ou référendum électronique seront situés dans une zone protégée, gardée en permanence contre des interférences de toutes sortes et de toutes personnes pendant la période du scrutin ou du référendum. Un plan de prévention des risques physiques sera mis en place pendant la période du scrutin ou du référendum. De plus, toutes les données conservées après la période du scrutin ou du référendum le seront en lieu sûr

Menace	Panne, blocage, site inaccessible Catastrophes naturelles → perte totale
Impact potentiel	Impact très important Perte totale de l'information
Vulnérabilité	Risque faible Il existe des normes et recommandations suivies notamment dans le domaine bancaire pour sécuriser l'information en cas de catastrophes naturelles, de crash d'avions, de champs électromagnétiques, …

Rec. 76

En cas d'incident susceptible d'affecter l'intégrité du système, les personnes chargées du fonctionnement de l'équipement en informeront automatiquement les autorités électorales compétentes, qui prendront les mesures nécessaires pour en atténuer les effets. Le niveau d'incident à signaler sera spécifié à l'avance par les autorités électorales.

Menace	En fonction de la gravité de l'incident…
	Panne, blocage, site inaccessible
	Catastrophes naturelles → perte totale
Impact potentiel	Impact très important
	Perte totale de l'information
Vulnérabilité	Risque faible
	Il existe des normes et recommandations suivies notamment dans le domaine bancaire pour sécuriser l'information en cas de catastrophes naturelles, de crash d'avions, de champs électromagnétiques, …

Sécurité… exigences générales…

Rec. 77

Des mesures techniques et organisationnelles seront prises pour s'assurer qu'aucune donnée ne sera définitivement perdue en cas de panne ou de défaut affectant le système de vote électronique.

Menace	Panne, blocage
Impact potentiel	Impact important
	Perte d'information
Vulnérabilité	Risque moyen
	Duplication de l'information réduit le risque (back-up)
	Mesures organisationnelles à prendre

Rec. 78

Le système de vote électronique préservera la vie privée des personnes. La confidentialité des listes électorales enregistrées ou communiquées par le système sera assurée.

Menace	Violation vie privée des personnes
Impact potentiel	Impact faible au niveau de l'élection
	Impact important au niveau du respect de la vie privée
Vulnérabilité	Risque faible
	Seules les informations strictement nécessaires sont gérées
	De plus, ces données sont sécurisées et ne sont accessibles que par des processus particuliers

Rec. 79

Le système de vote électronique vérifiera régulièrement la conformité aux spécifications techniques du fonctionnement de ses éléments et la disponibilité de ses services.

Menace	Panne, blocage
Impact potentiel	Impact important
	Perte d'information
Vulnérabilité	Risque moyen
	Utilisation de serveurs puissants réduit le risque
	Duplication de l'information réduit le risque (back-up)

Rec. 80

Le système de vote électronique restreindra l'accès à ses services, en fonction de l'identité de l'utilisateur ou de son rôle, aux services explicitement ouverts à cet utilisateur ou à ce rôle. L'identité de l'utilisateur sera établie avant toute action.

Menace	Utilisation frauduleuse de certains processus
Impact potentiel	Impact important
	Un expert informatique pourrait détourner les informations ou les manipuler
Vulnérabilité	Risque faible
	La gestion des droits d'accès est la base d'un service sécurisé

Rec. 81

Le système de vote électronique ou ses éléments protègeront les données d'authentification de manière à empêcher des entités non autorisées de détourner, d'intercepter, de modifier ou de prendre connaissance de toute autre manière de tout ou partie de ces données. Dans des environnements non contrôlés, il est recommandé de recourir à une authentification fondée sur la cryptographie.

Menace	Utilisation frauduleuse de certains processus
Impact potentiel	Impact important
	Un expert informatique pourrait détourner les informations ou les manipuler
Vulnérabilité	Risque faible
	La gestion des droits d'accès est la base d'un service sécurisé
	Utiliser des serveurs suffisamment puissants réduit le risque
	Cryptographie et autres processus de sécurité à mettre en place

Rec. 82

L'identification des électeurs et des candidats sera assurée d'une manière qui permette de les distinguer sans le moindre doute de toute autre personne (identification exclusive)

Menace	Usurpation d'identité, détournement de votes
Impact potentiel	Impact important
	Manipulation des suffrages
Vulnérabilité	Risque faible
	Gestion des accès via PKI

Sécurité... exigences pendant la période du scrutin...

Rec. 90

On garantira que le système de vote électronique présente un bulletin authentique à l'électeur. En cas de vote électronique à distance, l'électeur sera informé des moyens de vérifier que la connexion est établie avec le serveur authentique et qu'un bulletin authentique lui est présenté.

Menace	Phishing, usurpation d'identité, détournement de votes
Impact potentiel	Impact important
	Manipulation des suffrages
Vulnérabilité	Risque faible
	Gestion des accès via PKI
	Connexion sécurisée avec le serveur

Rec. 92

Des mesures suffisantes seront prises pour assurer la protection des systèmes utilisés par les électeurs pour exprimer leur suffrage contre des influences pouvant modifier leur décision.

Menace	Vote modifié
Impact potentiel	Impact réduit
	Manipulations, pressions
Vulnérabilité	Risque important (niveau physique)
	Impossible de garantir la confidentialité sans isoloir
	Risque faible (niveau logiciel)

Rec. 93

Les informations résiduelles qui renferment la décision de l'électeur ou l'image d'écran où s'affiche son choix seront détruites dès que le suffrage est exprimé. En cas de vote électronique à distance, l'électeur sera informé de la procédure à suivre pour effacer, si possible, les traces du suffrage exprimé de l'appareil utilisé pour enregistrer son suffrage.

Menace	Perte du secret / de la confidentialité du vote
Impact potentiel	Impact moyen
	Pressions, manipulations, vente de votes
Vulnérabilité	Risque faible (niveau logiciel)
	Risque important (niveau physique)
	Impossible de garantir la confidentialité sans isoloir
	Usage de l'appareil photo

Rec. 94

Le système de vote électronique vérifiera en premier lieu que l'utilisateur qui essaie de voter est habilité à le faire. Le système authentifiera l'électeur et s'assurera que seul le nombre approprié de suffrages par électeur sera enregistré et stocké dans l'urne électronique.

Menace	Usurpation d'identité, détournement de votes
	Plusieurs bulletins par électeur
Impact potentiel	Impact important
	Manipulation des suffrages
	Nombre de votes supérieur au nombre d'électeurs
Vulnérabilité	Risque faible
	Gestion des accès via PKI

Rec. 95

Le système de vote électronique garantira que la décision de l'électeur sera représentée avec exactitude dans le suffrage exprimé et que le vote scellé parviendra à l'urne électronique.

Menace	Modification du vote
	Suppression / détournement de vote
Impact potentiel	Impact important
	Manipulation des suffrages
	Nombre de votes inférieur au nombre d'électeurs
Vulnérabilité	Risque faible

Rec. 96

À l'issue de la période du scrutin électronique, aucun électeur n'aura accès au système de vote électronique. L'acceptation des suffrages électroniques dans l'urne électronique se poursuivra toutefois pendant un délai acceptable pour tenir compte des éventuels retards de transmission des messages au travers des différents modes de vote électronique.

Menace	Vote manquant
Impact potentiel	Impact important
	Nombre de votes inférieur au nombre d'électeurs
Vulnérabilité	Risque faible

Sécurité... exigences pendant la période post-électorale...

Rec. 97

L'intégrité des données communiquées pendant la période du scrutin (par exemple votes, inscription des électeurs, liste des candidats) sera préservée. L'origine des données sera authentifiée.

Menace	Perte d'informations
Impact potentiel	Impact important
	Résultats incorrects
Vulnérabilité	Risque faible
	Utilisation de serveurs puissants réduit le risque
	Duplication des données (back-up) réduit le risque

Rec. 98

Le dépouillement décomptera les voix avec précision. Il sera reproductible.

Menace	Erreurs dans le résultat
Impact potentiel	Impact important
Vulnérabilité	Risque faible
	Données toujours disponibles → décompte reproductible
	Décompte effectué grâce à un algorithme rigoureux (très bonne précision)

Rec. 99

Le système de vote électronique assurera, aussi longtemps que nécessaire, la disponibilité et l'intégrité des urnes électroniques et du résultat du dépouillement.

Menace	Pertes d'information
Impact potentiel	Impact important
Vulnérabilité	Risque faible
	Utilisation de serveurs puissants réduit le risque
	Duplication des données (back-up) réduit le risque

Après avoir analysé cette quarantaine de recommandations, nous pouvons, de manière générale, regrouper, l'ensemble de ces exigences selon 5 catégories.

1. Le choix de l'électeur est pris en compte une et une seule fois.

Menace	Nombre de votes différent du nombre d'électeurs
Impact potentiel	Impact important
Vulnérabilité	Risque faible

2. Le système garantit le secret du vote

Menace	Perte du secret du vote
Impact potentiel	Impact réduit (niveau physique)
	Impact important (niveau logiciel)
Vulnérabilité	Risque important en cas d'absence d'isoloir (niveau physique)
	Risque faible (niveau logiciel)
	Mesures prises au niveau logiciel

3. Le dépouillement peut être vérifié et exécuté à nouveau

Menace	Erreur ou contestation lors du dépouillement
Impact potentiel	Impact important
Vulnérabilité	Risque faible
	Les données restent disponibles pour un nouveau dépouillement

4. Mesures générales de sécurité (applicables pour d'autres systèmes informatiques également)

Menace	Fraude, panne, attaque en déni service
	Catastrophe naturelle, phishing
	Accès non sécurisé aux infrastructures
Impact potentiel	Impact important
Vulnérabilité	Risque faible

5. Le système exécute un contrôle d'identité

Menace	Usurpation d'identité
Impact potentiel	Impact important
Vulnérabilité	Risque faible

3.4.2 Objectif(s) de sécurité abordé(s)

Confidentialité	Le **vote** doit être **secret**, libre et anonyme (rec. 9, 11-12, 16-19, 34-35, 53-54, 78, 81, 93)
Intégrité	**Intégrité des données** (rec. 8, 34, 97, 99) **Intégrité du système** (rec. 29, 77, 92)
Authenticité	L'électeur doit s'identifier (rec. 16, 80-82, 94) Le système présente un bulletin authentique (rec. 90)
Disponibilité	Garantie de la disponibilité des services (rec. 30, 34, 70-72, 75, 79, 99)
Imputabilité	Le système ne conservera aucun lien entre le vote et l'électeur (rec. 17-18, 35, 51, 54, 93) Le résultat sera vérifiable (rec. 26, 51, 93, 98)
Non répudiation	Le vote ne pourra être modifié après enregistrement (rec. 15)
Fiabilité	Le système garantit que le choix de l'électeur sera correctement pris en compte (rec. 95) Le dépouillement décomptera les voix avec précision (rec. 8, 98)

3.5 Secret du vote – vérifiabilité du vote.

3.5.1 Préférence à la vérifiabilité du vote.

Sur base des éléments présentés dans le chapitre 2. Procédure de vote corporatiste par Internet, nous constatons que certaines élections corporatistes (vote aux AG d'une société cotée et élection du recteur de l'UCL) accordent beaucoup d'importance à la vérifiabilité du vote. Ceci permet notamment d'augmenter la confiance des électeurs dans le processus et de s'assurer que chaque vote a été correctement pris en compte. C'est d'ailleurs l'un des objectifs du projet HELIOS du professeur Ben Adida (Harvard), utilisé pour les élections du recteur de l'UCL.

Néanmoins, comme le mentionnait le professeur Adida, la vérifiabilité du vote entraîne une perte au niveau du secret du vote. En effet, pour pouvoir vérifier un vote, il est nécessaire d'avoir un signe distinctif, un identifiant, une référence qui permette d'identifier un vote en particulier. Si un vote est identifié en particulier, le secret du vote n'est plus garanti !

Nous sommes donc face à un dilemme : comment vérifier quelque chose qui est secret ? La seule possibilité est de voir s'il existe au moins un vote identique à celui de l'électeur qui tente de vérifier que son vote a correctement été pris en compte.

Une vérification très générale serait d'afficher, après le scrutin, l'ensemble des votes et de vérifier si on retrouve un vote correspondant. Il est évident que ce genre de preuves est très léger : ce n'est pas parce qu'il existe un vote identique à celui que cet électeur a émis que cet électeur a la certitude que son vote précisément a été pris en compte ! Néanmoins, à l'inverse, l'absence d'au moins un vote identique à celui de cet électeur permettrait clairement d'indiquer qu'il y a eu une erreur dans le processus de vote.

Pour avoir une preuve plus forte, il est indispensable d'utiliser certains systèmes, comme HELIOS, qui proposent des solutions de vérification de vote. Cependant, cela sera au détriment du secret du vote !

Comment cela se passe-t-il dans les élections sans Internet ?
Jusqu'il y a peu, certaines sociétés cotées utilisaient encore le vote à main levée lors de leurs assemblées générales. Le secret du vote était donc nul dès le moment de l'émission du vote. À contrario, la vérification était évidente !
À l'inverse, les élections pour le recteur de l'UCL, avant d'utiliser Internet, utilisaient des urnes traditionnelles (telles que nous le connaissons également pour les élections politiques). Via ces urnes, il était impossible de vérifier quoique ce soit au niveau de chaque vote. Dans ce genre de système, des urnes peuvent être perdues, les bulletins marqués (pouvant ainsi être vérifiés) sont déclarés nuls, ... Bref, la seule vérification possible était un recomptage des votes disponibles et acceptés comme valables ! Que faire pour les votes perdus, les votes marqués lors du dépouillement, ... ?

3.5.2 Préférence au secret du vote.

À l'inverse, sur base des éléments présentés dans le chapitre 2, nous constatons que d'autres élections corporatistes préfèrent maintenir la sécurité du vote à tout prix, peu importe la vérifiabilité. C'est le cas notamment des élections sociales.

Ce type d'élection repose sur le fonctionnement des urnes traditionnelles.

3.5.3 Absence d'isoloir.

L'analyse de risque met cependant en évidence un problème majeur des élections par Internet. Par définition, les votes pour ces élections peuvent être émis à partir de n'importe quel endroit, de n'importe quel PC relié à Internet, sans être nécessairement placé dans un isoloir. Dans cette optique, il est impossible de garantir le secret du vote puisqu'on ne peut pas garantir que l'électeur ne subit pas une quelconque pression au moment de l'émission de son vote. Même sans pression, l'électeur pourrait également faire une photo de son écran et ainsi prouver ultérieurement son vote. Bref, en l'absence d'isoloir, le secret du vote peut être perdu dès l'émission de celui-ci.

3.5.4 Secret du vote OU vérifiabilité du vote.

En conclusion, en fonction du type d'élection corporatiste par Internet étudié, le système informatique devra privilégier soit le secret du vote, soit la vérifiabilité du vote.

Il est évident que dans le cas où la vérifiabilité du vote est privilégiée, de nombreuses recommandations du Conseil de l'Europe ne pourront être satisfaites !

3.6 Objectifs de sécurité abordés

Une synthèse des différents objectifs de sécurité abordés conclut ce chapitre.

	PourEVA	Risque local à la machine « client » (Oppliger)	Recommandations du Conseil de l'Europe
Confidentialité	Le **secret du vote** est menacé		Le **vote** doit être **secret**, libre et anonyme (rec. 9, 11-12, 16-19, 34-35, 53-54, 78, 81, 93)
Intégrité		Il est difficile de garantir la sécurité de la machine « client » (**intégrité de la machine « client »**)	**Intégrité des données** (rec. 8, 34, 97, 99) **Intégrité du système** (rec. 29, 77, 92)
Authenticité			L'électeur doit s'identifier (rec. 16, 80-82, 94) Le système présente un bulletin authentique (rec. 90)
Disponibilité			Garantie de la disponibilité des services (rec. 30, 34, 70-72, 75, 79, 99)
Imputabilité	Le contrôle des opérations démocratiques n'est plus dans les mains du citoyen ou de l'électeur (**contrôle citoyen**)		Le système ne conservera aucun lien entre le vote et l'électeur (rec. 17-18, 35, 51, 54, 93) Le résultat sera vérifiable (rec. 26, 51, 93, 98)
Non répudiation			Le vote ne pourra être modifié après enregistrement (rec. 15)
Fiabilité			Le système garantit que le choix de l'électeur sera correctement pris en compte (rec. 95) Le dépouillement décomptera les voix avec précision (rec. 8, 98)

On peut compléter ce tableau avec les objectifs de sécurité abordés dans les différents exemples d'élections corporatistes étudiés au chapitre 2. Procédure de vote corporatiste par Internet.

	Elections sociales	Votes aux AG	Election du recteur de l'UCL	Election annuelle IEEE
Confidentialité	Le vote doit être secret	Le vote ne doit être secret que pour les questions ayant trait aux personnes (nomination ou révocation)	Le vote est chiffré	
Intégrité	Le système doit empêcher la modification du vote			
Authenticité	L'électeur reçoit son bulletin de vote sur présentation de sa convocation et de sa carte d'identité	Seuls les actionnaires présents dans la salle peuvent prendre part aux votes (exception : vote par procuration)	L'électeur s'identifie sur le portail du site de l'élection au moyen de son identifiant UCL et de son numéro de carte de membre (membre du personnel ou étudiant)	Chaque membre ayant le droit de voter reçoit un mail avec un lien pour se connecter au site des élections ; l'identifiant et le mot de passe de son compte Web IEEE lui permettent de s'identifier et ensuite de signer son vote
Disponibilité			Pour garantir la disponibilité du système de vote, il fut décidé de faire appel à des serveurs externes puissants (Amazon et Google)	

	Elections sociales	Votes aux AG	Election du recteur de l'UCL	Election annuelle IEEE
Imputabilité		Certains mandataires, pouvant représenter plusieurs actionnaires importants, peuvent recevoir la preuve qu'ils ont correctement émis la volonté des actionnaires qu'ils représentent	Ce système est appelé "open-audit" car l'audit complet de l'ensemble du processus est possible par tout observateur	

4 Modélisation des systèmes étudiés

Dans ce chapitre, une modélisation de chaque système étudié sera proposée.

Dans un premier temps, pour les élections n'utilisant pas encore Internet mais s'y préparant, la modélisation ne sera qu'une proposition de solution.

Dans un second temps, sur base des informations reçues pour les systèmes utilisant déjà Internet, la modélisation correspondra en effet au système effectivement mis en place.

Pour chaque modélisation, un lien avec les recommandations du Conseil de l'Europe, étudiées au chapitre précédent, sera établi.

4.1 Les élections sociales en Belgique.

4.1.1 Proposition de modélisation

Au sein des Facultés Universitaires Notre Dame de la Paix de Namur (FUNDP), la question de la sécurité sur le vote par Internet est étudiée depuis plusieurs années. En 2005, Francis Jeanmoye a réalisé son mémoire de fin d'étude sur la « *Sécurisation du vote électronique sur Internet* ».
Dans son mémoire, Monsieur Jeanmoye cherche à constituer un protocole qui permettrait d'assurer la sécurité du vote et de garantir le respect de 6 règles essentielles :

- seuls les électeurs autorisés peuvent voter
- personne ne peut voter plus d'une fois
- le vote d'un électeur doit être secret
- toute modification d'un vote doit être décelée
- tout électeur peut avoir la preuve que son vote a bien été pris en compte dans le décompte final
- il est possible de savoir qui a voté ou non

C'est ainsi qu'il arrive à proposer un protocole avec deux tiers de confiance :

- le 1er tiers de confiance vérifie que l'électeur a le droit de voter
- le 2^{e} tiers de confiance délivre un identifiant qui permettra de rechercher un vote en particulier

Néanmoins, ni l'électeur, ni les deux tiers de confiance ni l'organisateur de l'élection ne peuvent obtenir en même temps une information complète. Le secret du vote est ainsi garanti ! [Francis Jeanmoye, 2005]

Visiblement, le modèle proposé par Monsieur Jeanmoye répond à toutes les attentes réclamées par le système des élections sociales.

Expliquons en détail le modèle de Monsieur Jeanmoye.

Nous avons quatre entités :

- Electeur Elec
- Tiers confiance 1 Conf1
- Tiers confiance 2 Conf2
- Organisation responsable du vote Org

Nous utilisons cinq listes tout au long de ce processus :

- Liste des électeurs {Electeurs}
- Liste des votants {Votants}
- Liste des votes en cours {En_cours}
- Liste des votes {Votes}
- Liste des résultats {Résultats}

I. L'organisation responsable du vote établit la liste des électeurs comportant, pour chaque électeur,
   - son identification
   - sa clé publique

II. L'organisation responsable du vote transmet cette liste au 1er tiers de confiance, de façon chiffrée.

III. L'électeur émet son vote. Accompagné d'une variable, le vote est chiffré pour le 2e tiers de confiance. Le tout est signé par l'électeur. Avant de l'envoyer, ce message est chiffré pour le 1er tiers de confiance.
Seul le 2e tiers de confiance pourra déchiffrer le vote !

IV. Le 1er tiers de confiance déchiffre le message et vérifie que l'électeur est un électeur valide (présent dans la liste des électeurs mais pas dans celle des votants ou des votes en cours). Le 1er tiers de confiance vérifie également que l'électeur est bien l'auteur de ce message, en contrôlant sa signature

V. Le 1er tiers de confiance génère deux identifiants :
   a. Un pour l'électeur Ident1
   b. Un autre pour le 2e tiers de confiance Ident2

   Le 1er tiers de confiance envoie le vote chiffré au 2e tiers de confiance, accompagné de l'identifiant Ident2.
   Comme accusé de réception, le 1er tiers de confiance envoie un message à l'électeur, accompagné de l'identifiant Ident1.

   Les informations (identifiants, message de l'électeur) sont placées dans la liste des votes en cours pour éviter les doublons

VI. L'électeur déchiffre le message et reçoit son identifiant

VII. Le 2e tiers de confiance déchiffre le message et découvre l'identifiant
Ensuite, à l'intérieur du message reçu, il déchiffre le vote

VIII. Le 2e tiers de confiance génère un identifiant pour l'organisation responsable du vote, Ident3. Le vote et ce nouvel identifiant sont chiffrés et envoyés à l'organisation.
Les informations actuelles (vote, identifiants) sont placés dans la liste des votes.

IX. L'organisation déchiffre le message reçu et enregistre le vote ainsi que l'identifiant.
Un accusé de réception est ensuite envoyé au 2e tiers de confiance.

X. Le 2e tiers de confiance déchiffre le message reçu de l'organisation responsable du vote. Via l'identifiant de ce message, il retrouve le vote dans la liste des votes.
Il envoie alors un accusé de réception au 1er tiers de confiance.

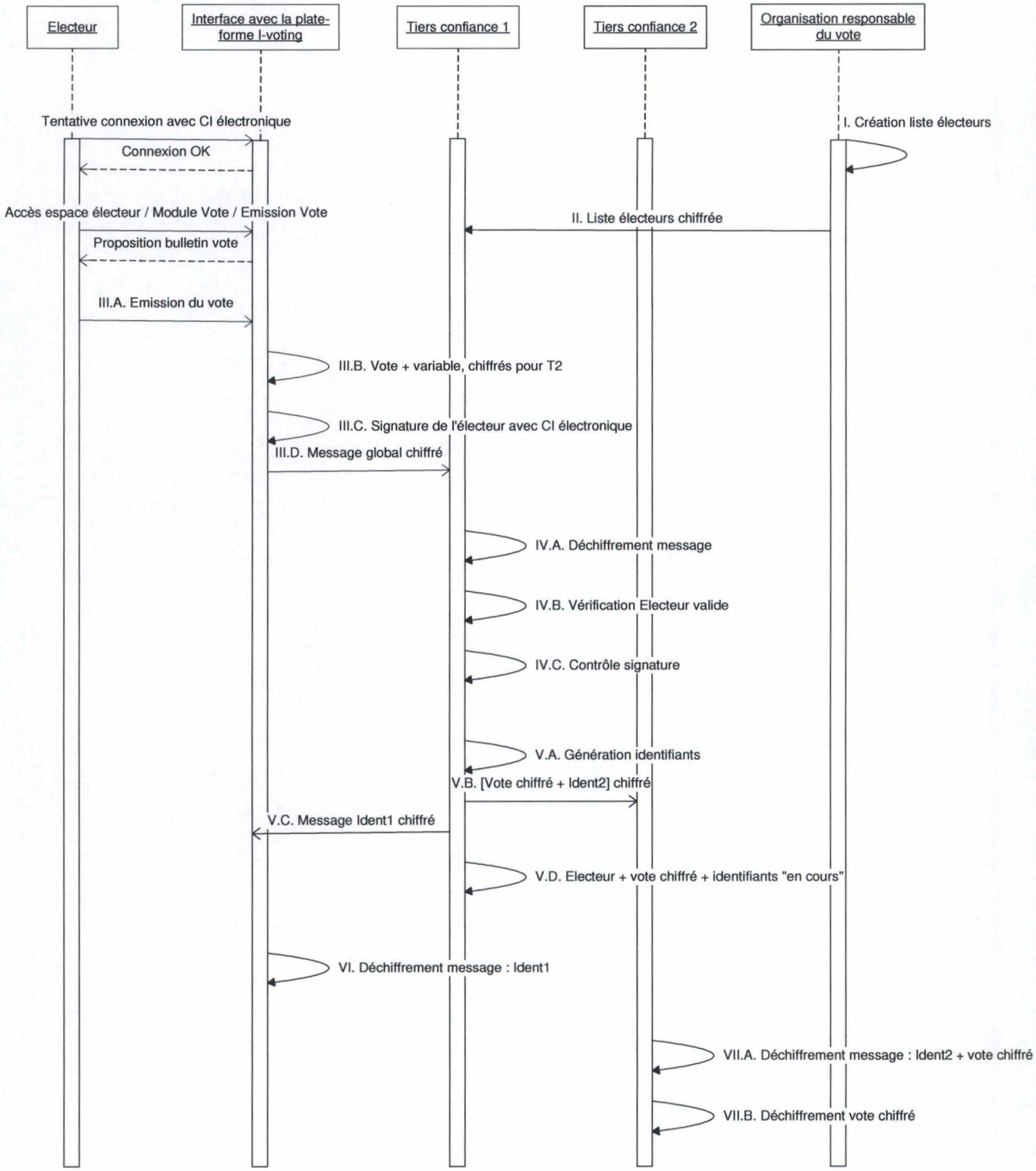
XI. Le 1er tiers de confiance déchiffre le message reçu du 2e tiers de confiance. Via l'identifiant, il retrouve les données correspondantes dans la liste des votes en cours et place ces informations dans la liste des votants.
De plus, dans la liste des participants à cette élection, on place l'électeur et son identifiant.

XII. Le 1er tiers de confiance confirme à l'électeur que son vote est accepté !

XIII. L'électeur déchiffre le message reçu du 1er tiers de confiance et constate que son vote a été pris en compte.

Aucune partie ne possède une information complète lui permettant de faire le lien entre l'électeur et son vote :

- L'électeur connaît
  - son **vote**
  - son **vote signé**
  - **Ident1**
- Le 1er tiers de confiance connaît
  - **l'électeur**
  - son **vote signé**
  - **Ident1**
  - **Ident2**
- Le 2e tiers de confiance connaît
  - le **vote**
  - le **vote signé**
  - **Ident2**
  - **Ident3**
- L'organisation responsable du vote connaît
  - le **vote**
  - **Ident3**


Electeur
Interface avec la plate-forme I-voting
Tiers confiance 1
Tiers confiance 2
Organisation responsable du vote
Tentative connexion avec CI électronique
Connexion OK
I. Création liste électeurs
Accès espace électeur / Module Vote / Emission Vote
II. Liste électeurs chiffrée
Proposition bulletin vote
III.A. Emission du vote
III.B. Vote + variable, chiffrés pour T2
III.C. Signature de l'électeur avec CI électronique
III.D. Message global chiffré
IV.A. Déchiffrement message
IV.B. Vérification Electeur valide
IV.C. Contrôle signature
V.A. Génération identifiants
V.B. [Vote chiffré + Ident2] chiffré
V.C. Message Ident1 chiffré
V.D. Electeur + vote chiffré + identifiants "en cours"
VI. Déchiffrement message : Ident1
VII.A. Déchiffrement message : Ident2 + vote chiffré
VII.B. Déchiffrement vote chiffré

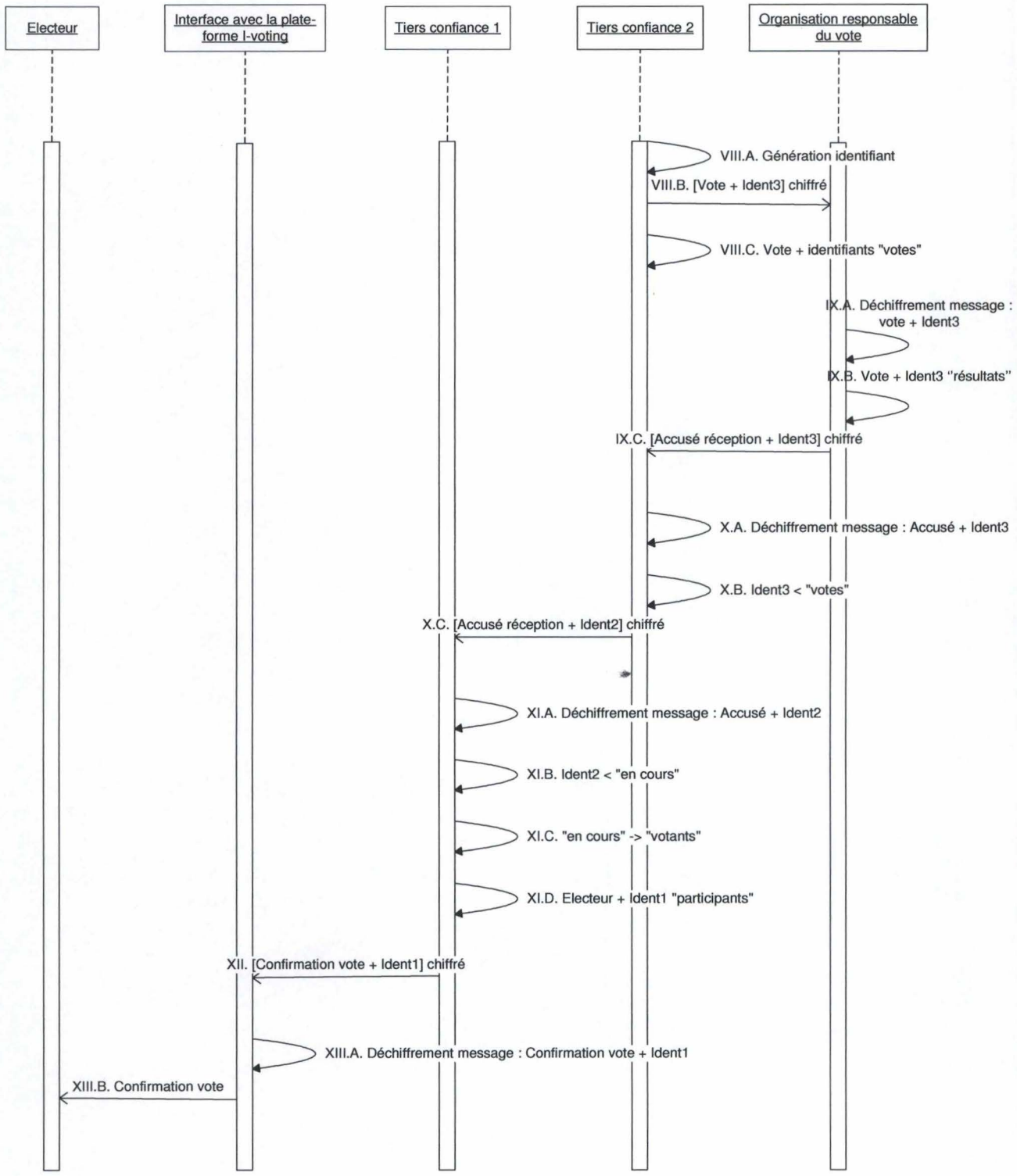


Figure 5 : Diagramme de séquence de la procédure de vote avec deux tiers de confiance

4.1.2 Observations par rapport aux recommandations étudiées

En passant le modèle proposé par Monsieur Jeanmoye dans le « filtre » des recommandations étudiées, nous constatons que ce modèle ne satisfait pas à plusieurs recommandations.

Il faut d'abord accepter que ce modèle ne s'intéresse qu'à la partie « émission du vote ». Il ne s'agit nullement d'un modèle appliqué dans la réalité et devant tenir compte de toutes les préoccupations organisationnelles.
Ceci explique que les recommandations 29, 30, 70, 71, 72, 74, 75, 76, 77, 79, 93, 96 ne sont pas supportées.

De plus, pour ce qui concerne les autres étapes du processus électoral, ce modèle ne donne aucune précision.
Par exemple,

- pour le transfert d'information entre la zone pré-élection et la zone élection ou entre la zone élection et la zone post-élection, aucune information n'est fournie concernant les candidats (rec. 97)
- le système ne s'occupe pas de l'identification des candidats (rec. 82)
- pour le dépouillement, aucune information n'est fournie (rec. 99)

De même, il y a plusieurs recommandations qui ne sont pas explicitement prises en compte mais pour lesquelles on peut imaginer facilement une solution.
Par exemple,

- lorsqu'il y a plusieurs modes de suffrage, il faut empêcher l'électeur de voter plusieurs fois (rec. 6, 44) : si la liste des votes en cours est commune pour tous les modes de suffrage, cela ne pose aucun problème
- lorsqu'il y a plusieurs modes de suffrage, il faut une comptabilisation correcte de tous les votes (rec. 8) : si le décompte est commun pour tous les modes de suffrage, cela ne pose aucun problème
- une modification du choix de vote, avant l'envoi et l'enregistrement (rec. 11) : ce modèle ne commençant qu'au moment de l'envoi du vote, cette recommandation n'est pas prise en compte ; néanmoins, rien n'empêche dans un processus global de permettre la modification jusqu'au moment où le vote est envoyé
- une modification du choix de vote, après l'enregistrement (rec. 15) : ce modèle ne donne aucune précision concernant la préservation des données dans l'urne ; néanmoins, on peut imposer que l'urne soit inaccessible jusqu'à la fin du scrutin
- le fait de bloquer l'accès à l'urne jusqu'à la fin du scrutin empêche par la même occasion des dépouillements partiels anticipés ; ce qui accepte la rec. 53
- le fait de bloquer l'accès à l'urne jusqu'à la fin du scrutin préserve la disponibilité et l'intégrité des suffrages (rec. 34)
- la possibilité de l'exécution d'un second dépouillement n'est pas précisé dans ce modèle (rec. 26, 98) ; néanmoins, on peut imposer que les votes restent disponibles dans l'urne.

Notons que même si on bloque l'accès à l'urne jusqu'à la phase de dépouillement, il serait intéressant de garder les votes chiffrés jusqu'à cette phase (rec. 55).

Si on considère que le vote s'effectue dans un environnement physique non sécurisé (sans isoloir), le problème du secret du vote se pose (rec. 9, 12, 16, 51, 92). Ce problème a déjà été abordé dans le chapitre 3.5.3. Absence d'isoloir.
Néanmoins, au niveau du modèle, tout est mis en œuvre pour garantir le secret du vote et la séparation électeur – vote (rec. 16) : voir explications dans l'observation finale du modèle.
De même, pour la confirmation du vote, le modèle n'offre qu'un accusé de confirmation (rec. 51) : voir explications étapes IX et suivantes

Enfin, pour terminer avec les points négatifs, notons que ce modèle n'offre pas la possibilité d'identifier l'électeur avant l'envoi du vote.
Cela pose différents problèmes :

- contrôle d'accès (rec. 80, 94)
- bulletin authentique (rec. 90) : quel bulletin offrir lorsqu'il y a plusieurs catégories d'électeurs comme c'est le cas pour les élections sociales ?

Une solution pour l'ensemble de ces 3 dernières recommandations serait de demander une identification avant l'envoi du vote.

Après avoir parcouru l'ensemble des points non supportés ou non précisés, nous pouvons constater que les recommandations au niveau de l'émission du vote sont supportées :

- rec. 5 : vérification via la liste des votes en cours (étape IV)
- rec. 17 : aucun lien entre vote et électeur sauf si les tiers de confiance échangent de l'information (observation finale du modèle)
- rec. 18, 54 : la liste des votes n'a aucun lien avec la liste des votants
- rec. 19 : seule la signature électronique est nécessaire mais il s'agit d'un code secret, privé (étape III)
- rec. 35 : séparation des données électeur – vote (étape V)
- rec. 78 : la liste des électeurs est transmise par l'organisation de l'élection au 1er tiers de confiance de façon chiffrée (étapes I et II)
- rec. 81 : la cryptographie est utilisée par ce modèle ; les données relatives aux électeurs sont stockées par un tiers de confiance
- rec. 95 : l'électeur reçoit un accusé de réception (étapes IX et suivantes).

4.2 Votes aux assemblées générales des sociétés cotées.

4.2.1 Proposition de modélisation

Une caractéristique importante de ce type de vote est que chaque vote a un poids différent en fonction du nombre d'actions qu'il représente.

Pour modéliser ce système, nous pouvons également utiliser le système de Monsieur Jeanmoye, avec la caractéristique supplémentaire que le nombre d'actions est renvoyé par le 1er tiers de confiance.

Au niveau du secret du vote, la plupart des votes n'ont pas besoin de garantir cette obligation, sauf en ce qui concerne les votes en rapport avec les personnes. Par contre, la vérifiabilité du vote est importante (sauf lorsque le vote doit être secret)…

Le système de Monsieur Jeanmoye convient parfaitement. Il suffit de permettre aux 2 tiers de confiance de communiquer entre eux lorsqu'il est nécessaire de vérifier le vote ou d'être totalement indépendant lorsque le vote doit être secret.

Puisqu'il s'agit de la même modélisation que le cas précédent, à la seule exception près du poids du vote en fonction du nombre d'actions déposées, la modélisation ne sera pas reprise explicitement une 2e fois (voir diagramme de séquence de la procédure de vote avec 2 tiers de confiance).

4.2.2 Observations par rapport aux recommandations étudiées

Au niveau des observations relatives au respect des recommandations étudiées, nous pouvons reprendre les mêmes que celles évoquées pour les élections sociales.

Par contre, pour les points concernant le secret du vote, ce type de vote permet justement, dans une certaine mesure que le secret ne soit pas garanti. Il est nécessaire que la confidentialité au moment de l'émission du vote soit garantie (on retrouve le même problème en cas d'absence d'isoloir) mais le vote ne doit pas nécessairement rester secret (possibilité de récupérer une preuve de son vote).
Dans ce cas bien précis, nous pouvons considérer que les recommandations du Conseil de l'Europe sont trop strictes pour ce type de vote !

4.3 L'élection du recteur de l'Université Catholique de Louvain.

4.3.1 Proposition de modélisation

Ce système repose sur le système HELIOS proposé par le professeur Ben Adida (Harvard).

Nous avons trois entités :

- Electeur — Elec
- Interface web - Valves Internet — Web
- Système — Syst

Tout le processus se déroule selon trois grandes étapes, telles que décrites au chapitre 2.2.1.2. Grille d'analyse selon 3 zones majeures.

A. Pré-élection
   - A.1. Inscription sur la liste des électeurs
   - A.2. Réception du code d'accès

B. Election : Vote

C. Post-élection : Dépouillement

I. L'électeur s'identifie sur le portail du site de l'élection au moyen de son identifiant UCL et de son numéro de carte de membre (membre du personnel ou étudiant)

II. Une demande de numéro d'électeur est faite au système qui renvoie ce numéro d'électeur à l'interface web. Ce numéro d'électeur doit être conservé par l'électeur.

III. L'électeur s'identifie sur le portail du site de l'élection au moyen de son identifiant UCL et de son numéro de carte de membre (membre du personnel ou étudiant)

IV. Une demande de code d'accès est faite au système qui renvoie ce code d'accès à l'interface web. Ce code d'accès doit être conservé par l'électeur.

V. L'électeur s'identifie sur le portail du site de l'élection au moyen de son identifiant UCL et de son numéro de carte de membre (membre du personnel ou étudiant)

VI. Après avoir reçu son bulletin de vote, l'électeur émet son vote.

VII. Le système envoie un numéro de suivi à l'interface web qui permettra à l'électeur de vérifier que son vote a bien été pris en compte.

VIII. L'électeur signe son vote avec son numéro d'électeur et son code d'accès.

IX. Le vote chiffré est envoyé vers le système.

X. Les informations relatives aux votes chiffrés sont affichées sur les valves Internet. L'électeur peut ainsi les consulter et, en cas de doute, peut recommencer la procédure de vote (point V.)

XI. Tous les votes chiffrés et anonymes sont regroupés sur le serveur pour le comptage des voix.

XII. Le dépouillement s'effectue sur le serveur via déchiffrement du résultat pondéré de l'élection.

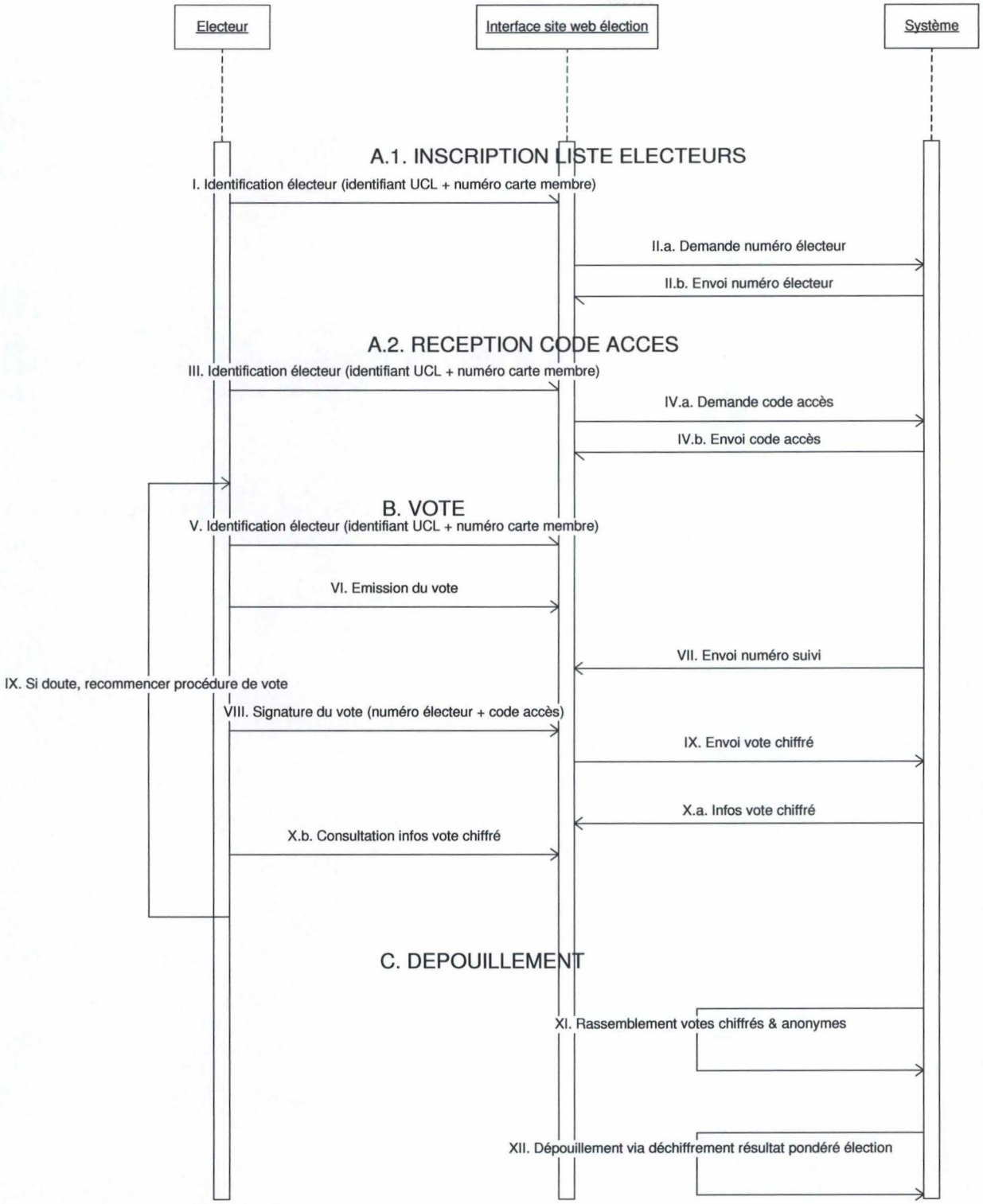


Figure 6: Diagramme de séquence de la procédure de vote utilisée pour l'élection du recteur de l'UCL

4.3.2 Observations par rapport aux recommandations étudiées

En passant le modèle de l'élection du recteur de l'UCL dans le « filtre » des recommandations étudiées, nous constatons que ce modèle satisfait à davantage de recommandations que le modèle précédent, même s'il en reste certaines qui ne sont pas prises en compte…

Toutes les préoccupations organisationnelles ne sont pas prises en compte (ou du moins pas détaillées). Ce qui explique que les recommandations 29, 70, 71, 72, 74, 76, 79, 93, 96 ne sont pas supportées.

Par contre, ce système a pris des mesures pour garantir la disponibilité du système (rec. 30, 75, 77) en utilisant des serveurs puissants extérieurs.

Si on considère que le vote s'effectue dans un environnement physique non sécurisé (sans isoloir), le problème du secret du vote se pose (rec. 9, 12, 16, 51, 92). Ce problème a déjà été abordé dans le chapitre 3.5.3. Absence d'isoloir.
Néanmoins, le système propose d'émettre un nouveau vote, qui supprimera le précédent. On peut donc supposer que l'électeur pourra émettre son vote sans influence et sans pression.
En ce qui concerne le lien entre le vote et l'électeur, le système offre juste un lien avec le vote chiffré.

Certaines informations ne sont pas précisées :

- la possibilité de 2^{e} dépouillement (rec. 26, 98) : on peut supposer que les votes restent disponibles pour un 2^{e} dépouillement
- la possibilité de vérification de l'authenticité du bulletin (rec. 90) : au cas où le bulletin n'est pas authentique, l'électeur ne retrouvera pas son vote sur les valves Internet ; il pourra émettre un nouveau vote
- les données communiquées pendant la période du scrutin sont préservées et l'origine authentifiée (rec. 97)
- le système assure la confidentialité des listes électorales (rec. 78) ; néanmoins, on peut supposer que ces données sont sécurisées.

D'un autre côté, plusieurs recommandations sont correctement suivies :

- l'électeur ne peut voter que par un seul mode de suffrage (rec. 6)
- l'électeur peut modifier son vote avant l'enregistrement de celui-ci (rec. 11)
- les votes restent scellés et anonymes jusqu'au dépouillement (rec. 34, 35, 54)
- le dépouillement (et le déchiffrement des votes) ne peut commencer que le lendemain de la fin du scrutin (rec. 53, 55)
- le système vérifie d'abord l'identité de l'utilisateur (rec. 80) et il n'y aura qu'un seul bulletin enregistré par électeur (rec. 94)

- les données d'authentification sont protégées et le système utilise une authentification fondée sur la cryptographie (rec. 81)
- l'électeur peut vérifier que son vote chiffré arrive dans l'urne (rec. 95).

Ce système veut proposer à l'électeur de vérifier que son vote a bien été pris en compte, via la présence de son vote chiffré sur les valves Internet. Si tel n'est pas le cas, le système permet à l'électeur d'émettre un nouveau vote ; ce qui supprimera automatiquement le vote précédemment enregistré.
Cela signifie qu'à la fin du scrutin, il n'y a au maximum qu'un seul bulletin par électeur dans l'urne électronique mais l'électeur aura pu, durant le scrutin, introduire plusieurs fois un bulletin.
Nous considérons que le terme « enregistrement du vote » est pris au sens « enregistrement définitif », à la fin du scrutin. Dans ce cas, les recommandations 5 – 7 – 15 sont correctement suivies.

D'autres recommandations ne s'appliquent pas pour ce système :

- il n'y a qu'un seul mode de suffrage (rec. 8, 44)
- l'identification distincte des électeurs et des candidats (rec. 82) : le système ne gère pas l'identification des candidats (seulement au nombre de 2, dans ce cas-ci).

4.4 L'élection annuelle de l'IEEE.

4.4.1 Proposition de modélisation

Par manque d'informations, aucun modèle ne peut être proposé pour l'élection annuelle de l'IEEE.

En effet, pour ma part, les questions relatives aux différentes étapes de ce processus électoral n'ont jamais trouvé de réponse précise. Comme mentionné au préalable, cette élection est sous-traitée à une société extérieure. Celle-ci est restée muette aux différentes tentatives d'information.

4.4.2 Observations par rapport aux recommandations étudiées.

Dans la même optique, l'absence d'informations, de détails et, par conséquent, de modélisation empêche la mise en rapport avec les recommandations étudiées.

4.5 Conclusion des propositions de modélisation et des observations par rapport aux recommandations étudiées.

4.5.1 Système de Monsieur Jeanmoye

Globalement, le système proposé par Monsieur Jeanmoye ne s'intéresse qu'à une partie bien précise : l'émission du vote jusqu'à la réception dans l'urne électronique.
Pour cette partie, les recommandations sont correctement suivies et ce modèle peut servir pour les élections sociales ainsi que pour le vote aux assemblées générales d'actionnaires.
Néanmoins, pour être utilisé dans la réalité, ce système doit être élargi en tenant compte des autres recommandations.

4.5.2 Système HELIOS

En ce qui concerne le modèle de l'élection du recteur de l'UCL, une bonne partie des recommandations sont suivies.
Les rares qui ne sont pas suivies concernent le secret du vote en cas d'absence d'isoloir mais la possibilité de voter à nouveau permettrait à l'électeur de voter sans pression extérieure. De plus, ce système prévoit que l'électeur peut vérifier que son vote chiffré est pris en compte.
Pour d'autres recommandations, on ne peut se prononcer

- soit parce qu'elles ne sont pas d'application dans ce contexte
- soit parce que nous n'avons pas suffisamment d'informations pour nous prononcer.

Globalement, le système HELIOS obtient de bons résultats par rapport aux recommandations.
De plus, les auteurs de ce projet (Ben Adida, Olivier de Marneffe, Olivier Pereira et Jean-Jacques Quisquater) ont reçu le « Best Paper Award » dans le cadre du meeting à Montréal « *2009 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE '09)* » pour leur article sur le déploiement du système HELIOS pour l'élection du recteur de l'UCL « *Electing a University President Using Open-Audit Voting :Analysis of Real-World Use of Helios* ». Cette récompense est une reconnaissance de la communauté scientifique dans le domaine par rapport à leur travail et la mise en œuvre du système HELIOS pour l'élection du recteur de l'UCL, soit une preuve supplémentaire de la qualité de ce système.
[Usenix, 2009]

Conclusion

Ce mémoire a abordé différentes élections corporatistes, chacune à des niveaux différents de l'utilisation d'Internet. Nous avons pu ainsi observer et analyser les différentes étapes essentielles pour le passage d'une élection traditionnelle vers une élection 100% online.

L'usage d'Internet pour les élections entraîne des risques. Ces risques ont été analysés selon les recommandations (très strictes) du Conseil de l'Europe. Ensuite, chacune des modélisations proposée a également été analysée selon ces mêmes recommandations.

Pour les élections sociales et le vote aux assemblées générales des actionnaires, la modélisation proposée est trop réduite sur la partie concernant l'émission du vote jusqu'à la réception du bulletin dans l'urne électronique. Les recommandations relatives au reste du processus électoral ne sont pas suivies mais il serait intéressant de voir ce modèle dans un cadre plus élargi.

Pour l'élection du recteur de l'UCL, la plupart des recommandations analysées ont été suivies. De plus, ce projet a reçu une reconnaissance de la part de la communauté scientifique.

Cependant, de façon globale, il faut nuancer ces résultats plutôt positifs. Deux grands problèmes viennent noircir le tableau :

- le secret du vote n'est pas respecté
- le risque sur la machine « client ».

En absence d'isoloir ou d'environnement sous surveillance, le secret du vote est menacé ! Cependant, dans le cadre des élections corporatistes, le secret du vote n'est plus nécessairement une obligation en soi. En effet, pour notamment augmenter la confiance des électeurs et leur donner la possibilité de vérifier le processus, certaines organisations ont choisi de privilégier la vérifiabilité du vote, au détriment du secret du vote.

Par contre, le risque sur la machine « client » n'est pas à négliger. Il est très difficile de garantir que l'émission du vote ne sera pas perturbée ou détournée par un logiciel malveillant résidant sur cette machine « client ».

En conclusion, je pense que l'I-voting peut proposer des solutions pour permettre aux électeurs de contrôler le déroulement des élections corporatistes tout en ayant la certitude que les systèmes évoqués respectent les règles en vigueur.

Néanmoins, pour permettre la poursuite du développement de l'I-voting pour les élections corporatistes, il est primordial de chercher une solution pour le risque sur la machine « client ».

Bibliographie

Ouvrages

Francis Jeanmoye, *Sécurisation du vote électronique sur Internet*, FUNDP, Namur, 2005

Articles

Agence Nationale de la Sécurité Informatique, La Norme ISO 13335, http://www.ansi.tn/fr/audit/norme_iso13335.htm, 2006, 30/8/2009

Ben Adida, Helios: Web-based Open-Audit Voting, http://www.usenix.org/events/sec08/tech/full_papers/adida/adida.pdf, 2009, 2/2/2009

CBFA, Avant-projet – Loi concernant l'exercice de certains droits des actionnaires de sociétés cotées, http://www.cbfa.be/fr/consultations/lop/pdf/2009-06-22_voorontwerp_avantprojet.pdf, 22/6/2009, 10/8/2009

CBFA, Consultation - Transposition de la Directive 2007/36, http://www.cbfa.be/fr/press/html/2009-06-22_consult.asp, 22/6/2009, 10/8/2009

Comité des Ministres du Conseil de l'Europe, *Recommandation Rec(2004)11 du Comité des Ministres aux Etats membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique*, http://www.coe.int/t/f/projets_integres/democratie/02_activit%E9s/02_vote_%E9lectronique/01_recommandation/00Rec(2004)11_FR.asp, 30/09/2004, 02/2008

Consortium de professeurs de KUL, UA, UG, UCL, ULg, ULB, VUB, *BeVoting Etude vote automatisé, Partie I, Version 1.1*, http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-1_fr.pdf, 15/04/2007, 02/2008

Consortium de professeurs de KUL, UA, UG, UCL, ULg, ULB, VUB, *BeVoting Etude des systèmes de vote électronique, Partie II, Version 1.02,* http://www.ibz.rrn.fgov.be/fileadmin/user_upload/elections_post_07/fr/presentation/bevoting-2_fr.pdf, 4/12/2007, 03/2008

guideinformatique.com, Sécurité des informations, normes BS 7799, ISO 17799, ISO 27001, EBIOS, MEHARI, http://www.guideinformatique.com/fiche-securite_des_informations-441.htm, 2009, 31/8/2009

IEC, Mission et objectifs, http://www.iec.ch/about/mission-f.htm, 2009, 30/8/2009

IEEE Bylaws, http://www.ieee.org/web/aboutus/whatis/bylaws/index.html, 2008, 14/3/2009

IEEE Policies, http://www.ieee.org/web/aboutus/whatis/policies/index.html, 2008, 14/3/2009

Mohamad Taghi Isaai, Fatemeh Firoozi, Mahmood Reza Hemyari, « E-election in Digital Society », 18/6/2009

Office for Democratic Institutions and Human Rights, *Republic Of Estonia - Parliamentary Elections - 4 March 2007 – OSCE / ODIHR Election Assessment Mission Report,* http://www.osce.org/documents/odihr/2007/07/25385_en.pdf, 28/06/2007, 07/2008

Pierre Escayez, « Le vote électronique, comment ça marche ? », *La Quinzaine*, Numéro 295, Page 7, 1/12/2008

Pierre Escayez, « Helios : un système « Made in Harvard » », *La Quinzaine*, Numéro 295, Page 7, 1/12/2008

PourEVA, Que voulons-nous ?, http://www.poureva.be/spip.php?article33, 2007, 16/08/2009

Région Wallonne, Thème « Technologies de l'information et de la communication (TIC) », http://atlas.wallonie.be/lexique/plan/recherche-et-technologie/technologies-de-l-information-et-de-la-communication-tic/, 2009, 30/8/2009

Dr Rolf Oppliger, *Traitement du problème de la sécurité des plates-formes pour le vote par Internet à Genève,* http://www.geneve.ch/evoting/doc/rapports/rapport_oppliger_fr.pdf, 03/05/2002, 03/2008

Service Public Fédéral Belge, Elections régionales et européennes, http://www.belgium.be/fr/la_belgique/pouvoirs_publics/democratie/elections/elections_regionales_et_europeennes/index.jsp, 2008, 13/08/2009

Service public fédéral Emploi, Travail et concertation sociale, Elections sociales 2008, http://www.emploi.belgique.be/electionssociales.aspx, 2008, 17/7/2009

Usenix, 2009 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections, http://www.usenix.org/event/evtwote09/tech/tech.html, 2009, 2/8/2009

Sites Internet

CBFA : http://www.cbfa.be

E-voting du Canton de Genève : http://www.geneve.ch/evoting/

Febelfin : http://www.febelfin.be

Organisation pour la sécurité et la coopération en Europe : http://fr.osce.org/

Pour une Ethique du Vote Automatisé (Vote Electronique) : http://www.poureva.be

Interviews

A.G., 27/7/2009, Entretien avec A.G., Responsable de l'organisation de l'assemblée générale des actionnaires d'une grande banque belge, Bruxelles, 2009

C.L., 19/8/2009, Echange de mails avec C.L., Responsable de l'organisation de l'élection annuelle de l'IEEE, 2009

D.C., 15/7/2009, Entretien avec D.C., Responsable Affaires Sociales au sein de la Febelfin, Bruxelles, 2009

J.J.Q., 28/1/2009, Echange de mails avec J.J.Q., Professeur en charge du système Helios, 2009

L.G., 10/8/2009, Entretien avec L.G., Responsable au sein du Service Juridique d'une grande banque belge, Bruxelles, 2009

O.P., 24/1/2009, Echange de mails avec O.P., Professeur en charge du système Helios, 2009

Annexes

Annexe 1 : interview d'un responsable des élections sociales au sein de la Febelfin.

Dans le cadre des élections sociales dans le domaine bancaire, j'ai contacté la Febelfin. Voici un bref compte-rendu de l'entretien avec Monsieur D.C.

Comment se déroulent les élections sociales en Belgique ?

Tous les quatre ans, un arrêté royal est publié pour établir les règles à respecter pour les élections sociales en Belgique.
Le SPF Emploi publie un guide pratique : http://www.emploi.belgique.be/electionssociales.aspx.
Vous y trouverez tous les renseignements nécessaires.

Pour le domaine bancaire notamment, la Febelfin est responsable de l'organisation de ces élections. Néanmoins, la marge de manœuvre est très faible.
Un groupe de travail paritaire (direction, syndicats) est créé au sein de l'entreprise (la banque en l'occurrence) pour la résolution de problèmes éventuels, en collaboration avec la Febelfin.

Actuellement, vous le savez certainement puisque vous travaillez dans une banque, ces élections se passent sous forme papier.

Existe-t-il un projet pour utiliser Internet pour les élections sociales ?

Cette idée est soutenue par l'ensemble des directions des grandes banques belges. A l'heure où nous utilisons de plus en plus Internet pour nos opérations bancaires, l'idée d'utiliser également Internet pour les élections sociales voit progressivement le jour, dans le domaine bancaire principalement.

Les avantages tirés de l'utilisation d'Internet seraient, par exemple :

- *gain de temps*
- *gain de productivité*
- *rapidité de dépouillement*

Malheureusement, actuellement, rien n'est encore prévu à ce niveau..

Pour 2012, on réfléchit à l'idée d'informatiser les élections sociales (vote électronique).

La crainte du risque de fraudes ralentit quelque peu les ardeurs.
Au niveau des syndicats, ils ne sont pas contre l'idée mais ils désirent des garanties sur le secret du vote qui est primordial !

La réflexion se fait au niveau de la Fédération Belge des Entreprises (FEB) mais vous comprendrez aisément que la crise économique actuelle prime sur les autres préoccupations.

Avez-vous déjà établi un référentiel des contraintes à respecter pour le vote par Internet ? Ou savez-vous quel(s) référentiel(s) sera(seront) utilisé(s) ?

Il n'y a pas encore, à ma connaissance, de référentiel établi à ce niveau. L'idée n'est pas suffisamment approfondie.

D'autres grandes banques sont également demandeuses.

Les banques pourraient proposer un projet pilote avec vérification pour un nombre limité de votes.

Annexe 2 : calendrier pour les élections sociales en Belgique, dans le domaine bancaire

- 60 jours avant l'affichage de la date des élections : premières informations écrites
  - détermination du nombre de membres du personnel par catégorie de travailleurs
  - fonctions cadres et liste indicative des cadres
  - fonctions de personnel de direction et liste indicative du personnel de direction
  - proposition de date pour l'affichage de la date des élections et de la date des élections proprement dite
- entre 60 jours et 35 jours avant l'affichage de la date des élections : consultation
  - la direction consulte le comité, le conseil ou les délégations syndicales sur les informations fournies précédemment
- 35 jours avant l'affichage de la date des élections : communication écrite des décisions
- entre 35 jours et 28 jours avant l'affichage de la date des élections : recours contre ces décisions
- entre 28 jours et 5 jours avant l'affichage de la date des élections : jugement du tribunal du travail saisi sur base des recours
- 90 jours avant le jour de l'élection : affichage de la date des élections
  - date et horaire de l'élection
  - nombre de mandats par conseil ou comité et par catégorie
  - listes électorales provisoires ou lieu où elles peuvent être consultées
  - liste des cadres
  - liste des membres du personnel de direction
- 35 jours après l'affichage de la date des élections : introduction des listes de candidats
  - conditions d'éligibilité
    - âgé 18 ans au moins et moins 65 ans
    - non membre du personnel de direction
    - pas conseiller en prévention du SIPP
    - conditions d'ancienneté
- de 35 jours à 40 jours après l'affichage de la date des élections : candidatures
  - attribution des numéros de liste
  - affichage des listes de candidats
- de 40 jours à 70 jours après l'affichage de la date des élections : constitution des collèges électoraux
  - un collège électoral de jeunes travailleurs n'est créé que s'il existe au moins 25 électeurs de moins de 25 ans
- 77 jours après l'affichage de la date des élections : clôture des listes de candidats et confection des bulletins de vote
- 80 jours après l'affichage de la date des élections : convocations des électeurs
  - envoi ou remise des convocations
  - envoi des bulletins pour le vote par correspondance
- 90 jours après l'affichage de la date des élections : opération de vote

Annexe 3 : interview d'une responsable de l'organisation de l'assemblée générale des actionnaires d'une grande banque belge

Dans le cadre des votes aux assemblées générales des actionnaires de sociétés cotées, j'ai pris contact avec le service qui organise l'assemblée générale pour la grande banque belge pour laquelle je travaille. Voici un bref compte-rendu de l'entretien que j'ai eu avec Madame A.G.

Comment se passe une assemblée générale dans notre banque ?

L'assemblée générale pour notre banque se déroule toujours le 2e mercredi du mois de mai.

Les actionnaires qui ont rempli une série de conditions peuvent assister à l'assemblée générale et, au moment des votes, émettre leur opinion à l'aide d'un boîtier électronique. Seuls les actionnaires présents physiquement dans la salle peuvent voter. Il existe aussi un système de procuration, soit à une personne soit au Président.

L'assemblée générale est retransmise en direct sur Internet mais l'actionnaire internaute ne peut pas voter à distance, sauf s'il a donné procuration au préalable.

Quand et comment les convocations sont-elles envoyées ?

L'assemblée générale est annoncée par différents canaux (presse écrite spécialisée, site web de la banque, sites web financiers, etc.)

Les actionnaires dont les actions sont déposées dans le Grand Livre des actionnaires reçoivent une invitation personnelle.

Les actionnaires détenant leurs actions au porteur ne reçoivent pas d'invitation personnelle.

Quelles sont les conditions à remplir pour pouvoir voter ? Tout actionnaire ne peut pas assister à l'assemblée générale ?

Tout actionnaire peut bien sûr assister à l'assemblée générale et voter lorsque c'est nécessaire. Peu importe le nombre d'actions qu'il détient ! Sa voix compte pour autant d'actions qu'il détient, ou plutôt qu'il a déposées.

En effet, l'actionnaire qui désire assister à l'assemblée générale doit, au préalable, déposer ses actions plusieurs jours à l'avance et jusqu'à la fin de l'assemblée générale. En d'autres termes, durant cette période, il ne pourra pas vendre ses actions.

Il reçoit alors une invitation (cfr. convocation) qui lui permet d'accéder à la salle le jour de l'assemblée générale.

L'invitation, reprenant le nombre d'actions en dépôt, accompagnée de la carte d'identité de l'actionnaire permet de réaliser l'inscription le jour même de l'assemblée générale. L'actionnaire reçoit alors un boîtier électronique pour le vote et une carte à puce reprenant le nombre d'actions déposées pour cet actionnaire. Cela permet de faire le lien entre l'actionnaire et le nombre d'actions qu'il représente, au moment du vote.

Ces informations sont conservées dans une base de données, au cas où l'actionnaire perdrait sa carte durant l'assemblée générale. Cela nous permet d'annuler la carte précédente et de lui rendre une nouvelle carte avec le nombre correct d'actions déposées.

Comment se déroule un vote ?

Au moment du vote, il existe une procédure spécifique :

- *le Président de l'assemblée générale énonce la question*
- *il ouvre la période de vote*
- *les actionnaires ont le temps nécessaire pour voter*
- *le Président s'assure que tout le monde a eu l'occasion de voter*
- *il clôt la période de vote*
- *les résultats s'affichent*

Seuls des résultats globaux sont affichés :

- *POUR*
- *CONTRE*
- *ABSTENTION*

Ces résultats sont exprimés en pourcentage et en nombre d'actions.

Le vote est-il secret ?

Au moment du vote, l'actionnaire émet son opinion à l'aide de son boîtier électronique. A part ses voisins directs, personne ne peut connaître son vote.

Mais vous dites que le lien actionnaire – nombre de voix – référence de la carte à puce est conservée. Vous pouvez donc retracer le choix de chaque actionnaire ?

Pour ces questions plus précises, je vous suggère de vous adresser au service juridique.

Notez que dans une autre grande banque belge, il y a 2-3 ans d'ici, le vote se faisait à main levée pour ceux qui étaient contre la résolution. Il n'y avait donc aucun secret du vote.

Je pense que cela dépend des statuts de la banque. Le plus simple est certainement de contacter le service juridique.

Qui peut soumettre une question au vote des actionnaires ?

Les questions et résolutions sont généralement proposées par le Conseil d'Administration. Pour des détails complémentaires, je vous renvoie également auprès du service juridique.

Existe-t-il un projet d'utiliser Internet pour les votes lors d'une assemblée générale ?

À ma connaissance, non !
L'assemblée est retransmise sur le site de la banque mais l'actionnaire internaute ne peut pas voter à distance, sauf s'il a donné procuration au préalable.

Il faut noter que durant la retransmission sur Internet, toute intervention d'un actionnaire est audible mais l'actionnaire n'est pas filmé ! Pour le respect de la vie privée, la caméra reste toujours fixée sur le Président ou sur les résultats mais jamais sur les actionnaires

Annexe 4 : interview d'une responsable du service juridique d'une grande banque belge

Dans le cadre des votes aux assemblées générales des actionnaires de sociétés cotées et en vue de compléter les informations reçues lors de l'entretien eu avec Madame A.G., j'ai pris contact avec le service juridique de la grande banque belge pour laquelle je travaille. Voici un bref compte-rendu de l'entretien que j'ai eu avec Madame L.G..

J'ai déjà eu quelques explications sur le déroulement de l'assemblée générale, grâce à Madame A.G. Néanmoins, il reste certaines questions en suspens…

Le vote est-il secret ? Ou, au contraire, est-il possible de vérifier qui a voté dans quel sens ?

A la base, le droit des sociétés indique que le vote doit être secret uniquement pour les questions concernant les personnes (nomination ou révocation).

De plus, en cas de litige, il faut pouvoir vérifier.
Nous recevons parfois des demandes de mandataires (pouvant représenter plusieurs actionnaires importants) pour obtenir la preuve qu'ils ont bien voté dans le sens demandé par les actionnaires qu'ils représentent. Néanmoins, nous ne donnons pas d'informations sur les choix d'un autre actionnaire…

En pratique donc, le vote n'est pas secret, au sens juridique du terme. Une certaine liberté statutaire est laissée pour les votes aux assemblées générales.

Qui peut soumettre une question ou une résolution au vote des actionnaires ?

Généralement, les questions et résolutions sont soumises soit par le Conseil d'Administration, soit par les commissaires.
Néanmoins, les actionnaires représentant au minimum 20% du capital peuvent soumettre des questions ou résolutions.

L'ensemble des questions sont reprises dans un livret qui accompagne l'invitation.

Est-il possible de consulter la liste des actionnaires pour pouvoir savoir qui vote ?

Au sein de notre société, le respect de la vie privée est primordial ! Nous ne publions pas d'informations sur les actionnaires.

D'ailleurs, lorsqu'on filme l'assemblée générale pour la retransmission sur Internet, les actionnaires ne sont jamais filmés. La caméra reste sur le Président du Comité de Direction ou sur le Président du Conseil d'Administration et, au moment de la publication des résultats, sur ceux-ci !

Seule exception, pour une assemblée générale extraordinaire, la liste des « électeurs » est chez le notaire !

Existe-t-il un projet d'utiliser Internet pour les votes lors d'une assemblée générale ?

Oui, une directive européenne a été prise dans ce sens. Un avant-projet de loi est actuellement à l'étude au sein de la Commission Bancaire, Financière et des Assurances (CBFA).

Cela permettrait à l'actionnaire qui regarde l'assemblée générale sur Internet de pouvoir voter. C'est intéressant pour les sociétés dont l'actionnariat est réparti à travers le monde ou plusieurs pays.

Néanmoins, la procédure actuelle de dépôt des actions au préalable pose un problème si on veut pouvoir voter par Internet. Dans la même optique, l'identification de l'actionnaire pourrait poser un certain nombre de problèmes de sécurité.

Annexe 5 : échange de mails avec le professeur O. P. (élection du recteur de l'UCL)

Monsieur,

Étudiant en informatique aux Facultés Universitaires Notre Dame de la Paix (FUNDP) à Namur, je réalise mon mémoire sur la sécurité du vote électronique par Internet (promoteurs : Prof. Ramaekers et Schumacher).
En fait, je m'intéresse à différents processus de vote utilisés actuellement et je tente de les analyser sur différents points :

- émission du vote (cryptographie, possibilités de voter plusieurs fois, lien électeur - vote, ...)
- stockage du vote
- dépouillement du vote
- vérification de l'élection
- référentiel de contraintes (Recommandations du Conseil de l'Europe, par exemple)
- ...

Dans cette optique, je me suis intéressé aux élections pour le Recteur de l'Université Catholique de Louvain (UCL) et j'ai lu un article concernant le projet HELIOS (La Quinzaine N° 295). Cet article explique globalement comment se passe le processus de vote.

Fortement intéressé par le sujet et ayant quelques questions en rapport avec cet article, je me permets de vous contacter.
Pourriez-vous me renseigner ou me transmettre une documentation plus approfondie sur ce projet HELIOS?

Merci d'avance!

Bien à vous,

Michael Maréchal

PS : Quelques questions qui surgissent au moment de la lecture de l'article :

- Comment est gérée la possibilité offerte à l'électeur de voter plusieurs fois? Comment retrouve-t-on son précédent vote qui doit être supprimé avant de prendre en compte son nouveau vote, puisqu'il semble n'y avoir aucun lien entre l'électeur et le vote (code accès non stocké)?
- Quel référentiel de contraintes utilisez-vous pour ces élections? L'impression à différentes étapes du processus pourrait laisser la porte ouverte à l'absence ou la suppression du secret du vote impliquant des ventes de vote, des pressions, etc. (peut-être pas dans le cadre de cette élection mais ce système serait-il transférable vers d'autres types d'élections (législatives, par exemple))?
- Quelle preuve pouvez-vous fournir que les résultats finaux correspondent bien à l'ensemble des votes des électeurs? Contrôle à posteriori OK mais rien au moment même du dépouillement... Quelle garantie a-t-on qu'on utilise bien les bons votes et pas de nouveaux introduits frauduleusement?
- ...

PS (2) : Je tiens à préciser que ces questions ne cherchent qu'à répondre aux différents critères de l'analyse que je réalise sur différents systèmes de vote.

Bonsoir,

Merci pour cette marque d'intérêt! Je serai certainement heureux de découvrir les conclusions de vos analyses!

Vous trouverez une description du système Helios dans l'article <http://www.usenix.org/events/sec08/tech/full_papers/adida/adida.pdf>. Le système a assez bien évolué depuis lors du point de vue technique (l'évolution principale étant de baser le décompte sur du chiffrement homomorphique plutôt que sur des mixnets), mais les principes restent les mêmes.

Par ailleurs, vous pouvez étudier le code d'Helios sur <http://github.com/benadida/helios/> . Ce code a beaucoup évolué pour répondre aux besoins de l'UCL, en collaboration avec Ben Adida. Nous nous servons de la branche django. Beaucoup de choses ont bien sûr aussi été développées à l'UCL, pour les besoins de l'élection qui nous occupe.

Concernant vos questions:

> PS : Quelques questions qui surgissent au moment de la lecture de l'article :
> - Comment est gérée la possibilité offerte à l'électeur de voter
> plusieurs fois? Comment retrouve-t-on son précédent vote qui doit
> être supprimé avant de prendre en compte son nouveau vote, puisqu'il
> semble n'y avoir aucun lien entre l'électeur et le vote (code accès
> non stocké)?

Le lien entre le numéro d'électeur et le vote est conservé à tout moment, et affiché sur les valves internet. Ce sont les mots de passe que nous ne stockons que sous forme hashée (nous voulions avertir les électeurs que nous ne leur rendrons pas leur mot de passe s'ils le perdent - nous n'en avons qu'un hash.)

> - Quel référentiel de contraintes utilisez-vous pour ces élections?
> L'impression à différentes étapes du processus pourrait laisser la
> porte ouverte à l'absence ou la suppression du secret du vote
> impliquant des ventes de vote, des pressions, etc. (peut-être pas
> dans le cadre de cette élection mais ce système serait-il
> transférable vers d'autres types d'élections (législatives, par
> exemple))?

On n'imprime que des hashes de bulletins de vote chiffrés. La seule chose à laquelle ces documents peuvent réellement servir si ils sont divulgués est de vérifier si une personne a (re-)voté ou non. Nous n'envisageons pas de répondre sérieusement aux préoccupations concernant la vente de vote ou le vote sous contrainte: la chose est essentiellement impossible si on ne force pas l'électeur à s'isoler un moment, ce que l'UCL ne souhaitait pas imposer.

Je m'opposerais clairement à l'usage d'un système comme Helios pour des élections dans lesquelles le vote sous contrainte ou la vente de vote est une préoccupation. (Et Ben Adida, l'auteur d'Helios, est clairement de cet avis aussi.)

- Quelle preuve pouvez-vous fournir que les résultats
> finaux correspondent bien à l'ensemble des votes des électeurs?
> Contrôle à posteriori OK mais rien au moment même du dépouillement...
> Quelle garantie a-t-on qu'on utilise bien les bons votes et pas de
> nouveaux introduits frauduleusement? - ...

Les votes chiffrés sont publics, ainsi que leur hash. Chaque électeur est invité à vérifier que le hash affiché sur les valves internet (et signé par la Commission électorale) correspond bien à celui qu'il a imprimé (ou noté, ou ...) lorsqu'il a voté. Par ailleurs, toute personne ayant les compétences nécessaires peut vérifier que tous les hashes affichés sont bien les hashes des votes chiffrés qui sont publiés eux aussi.

Ceci a pour but de garantir, avant que le décompte ne commence, que les votes affichés sur les valves internet sont les bons. La Commission électorale, qui connaît la correspondance entre numéros d'électeurs et électeurs, peut par ailleurs s'assurer que chaque numéro d'électeur correspond réellement à un électeur.

Nous nous attendons bien à ce que tout le monde ne vérifie pas son vote sur les valves internet. Cependant, nous ne savons pas d'avance qui vérifiera, et toute modification conséquente de votes a dès lors une forte probabilité d'être détectée.

Ensuite, lors du dépouillement, chaque porteur de clé fournit une preuve (zero knowledge) qu'il a correctement effectué sa tâche. N'importe qui, ayant accès à l'ensemble des bulletins de vote chiffrés, peut donc techniquement vérifier que le résultat du dépouillement est bien conforme à l'ensemble des votes qui étaient repris sur les valves.

La vérification publique a donc lieu en deux temps:
- nous souhaitons qu'un maximum de personnes vérifient les hashes signés de leur bulletin de vote, publiés sur les valves internet, et ce avant le décompte
- nous publions ensuite la preuve que le décompte est bien conforme à ce qui se trouvait sur les valves; et nous nous attendons à ce que l'une ou l'autre personne vérifie que ce décompte a été effectué correctement

> PS (2) : Je tiens à préciser que ces questions ne cherchent qu'à
> répondre aux différents critères de l'analyse que je réalise sur
> différents systèmes de vote.

Ce sont des questions qui me semblent très naturelles!
J'espère avoir déjà pu clarifier certaines choses,

Au cas où vous seriez intéressé, Ben Adida donnera le cours de cryptographie du mardi 3 février à 16h15 à l'UCL, sur le vote électronique. Vous êtes bien sûr le bienvenu!

Bien cordialement,

O. P.

Annexe 6 : échange de mails avec le professeur J.J.Q. (élection du recteur de l'UCL)

Monsieur,

Étudiant en informatique aux Facultés Universitaires Notre Dame de la Paix (FUNDP) à Namur, je réalise mon mémoire sur la sécurité du vote électronique par Internet (promoteurs : Prof. Ramaekers et Schumacher).
En fait, je m'intéresse à différents processus de vote utilisés actuellement et je tente de les analyser sur différents points :

- émission du vote (cryptographie, possibilités de voter plusieurs fois, lien électeur - vote, ...)
- stockage du vote
- dépouillement du vote
- vérification de l'élection
- référentiel de contraintes (Recommandations du Conseil de l'Europe, par exemple)
- ...

Dans cette optique, je me suis intéressé aux élections pour le Recteur de l'Université Catholique de Louvain (UCL) et j'ai lu un article concernant le projet HELIOS (La Quinzaine N° 295). Cet article explique globalement comment se passe le processus de vote.

Fortement intéressé par le sujet et ayant quelques questions en rapport avec cet article, je me permets de vous contacter.
Pourriez-vous me renseigner ou me transmettre une documentation plus approfondie sur ce projet HELIOS?

Merci d'avance!

Bien à vous,

Michael Maréchal

PS : Quelques questions qui surgissent au moment de la lecture de l'article :

- Comment est gérée la possibilité offerte à l'électeur de voter plusieurs fois? Comment retrouve-t-on son précédent vote qui doit être supprimé avant de prendre en compte son nouveau vote, puisqu'il semble n'y avoir aucun lien entre l'électeur et le vote (code accès non stocké)?
- Quel référentiel de contraintes utilisez-vous pour ces élections? L'impression à différentes étapes du processus pourrait laisser la porte ouverte à l'absence ou la suppression du secret du vote impliquant des ventes de vote, des pressions, etc. (peut-être pas dans le cadre de cette élection mais ce système serait-il transférable vers d'autres types d'élections (législatives, par exemple))?
- Quelle preuve pouvez-vous fournir que les résultats finaux correspondent bien à l'ensemble des votes des électeurs? Contrôle à posteriori OK mais rien au moment même du dépouillement... Quelle garantie a-t-on qu'on utilise bien les bons votes et pas de nouveaux introduits frauduleusement?
- ...

PS (2) : Je tiens à préciser que ces questions ne cherchent qu'à répondre aux différents critères de l'analyse que je réalise sur différents systèmes de vote.

Bonjour,

Merci pour votre message et votre intérêt.

Le projet helios se trouve en
http://www.heliosvoting.org/
(v-lire la FAQ et le blog).

Ce système n'est pas prévu pour être utilisé dans le contexte d'élections législatives de notre point de vue.

Voir aussi le papier d'usenix :
http://www.usenix.org/events/sec08/tech/full_papers/adida/adida.pdf
(le système a été amélioré depuis lors).

Nous sommes en plein dans le feu de l'action et vos questions sont pertinentes. Nos sommes prêts à répondre à vos questions mais un peu plus tard (je rentre d'un voyage de 2 semaines au Pérou et au Chili).

Le concepteur du système, Ben Adida (Harvard) sera à l'UCL la semaine prochaine : je vous tiens au courant de ses exposés.

Cordialement,

J.J.Q.

Annexe 7 : échange de mails avec C.L. (IEEE)

Hello,

In the framework of my thesis on the security of electronic voting, I'm looking at several existing systems.
Your association drew my attention, given the recognition it has already received in the computer world.
Could I therefore ask you to give me some details on the technical mechanisms in practice fort the elections in your association?
I would be grateful if you could explain to me the different steps of the elections, the security aspects, the different intermediaries (server, third party, ...)?

Looking forward to receiving the information, an thanking you in advance,

Your faithfully,

Michael Maréchal
Student in Notre Dame de la Paix University (FUNDP) - Namur (Belgium)

Mr. Marechal:

My apologies for the late reply. Your email went to the SPAM box.

The IEEE annual election uses an outside firm to manage the creation of the ballot, all the printing and the electronic ballot access. We have two electronic authentication options. One is the use of the IEEE Web Account username and password and the election vendor assigned unique Control Number and E-signature. Members go to the election vendor ballot site https://www.directvote.net/ieee/ and select the electronic authentication method. If the member uses an IEEE Web Account, when they click on the link, it will take them to the IEEE to a customized authentication page. Once the authentication is successful, a CID cookie is transmitted back to the vendor, the vendor's server will receive the authentication key and let the member access his/her unique ballot.

If a member mails in the paper ballot, the election vendor will scan the ballot and store the data in the same database. The ballot that is first received is counted. This is to avoid double submission by a member.

Another tool that IEEE has for some smaller scale elections is vTools. I am not involved with that project but you can find some information at http://wiki.vtools.ieee.org/bin/view/Voting/WebHome.

Again, my apologies for the late reply. Please let me know if you are looking for more details.

Sincerely,

C. :)

C.L.
IEEE Annual Election

Dear C.,

Many thanks for your reply.

I have further questions relating to the IEEE election.

Which outside firms are managing the election ?
I thought it was managed by Intelliscan (firm that I tried to contact to have some information but without any success). My emails are maybe sent as well in the SPAM Box.
Do you know by any chance a contact person there that could help me with my thesis ?
Could you please send them our exchange of mails and see if they can help me ? If not possible, could you please send me the email adress of one person that is working in that firm that could help me.

In the anwser provided by you, you are describing the full process of the identification but I'd like to know how it is working after that. For example, could you please explain the full voting process ?

Here are some specific questions for the voting process :

I guess the vote is encrypted, but when and how is it done ?
Is the server that receives the vote the same than the one that manages the voters list ?

In Europe, vote must be secret. Do you guarantee it during your elections ?

How do you manage the voters list ?
How are the votes stocked ? How are they decrypted ?
How do you guarantee the anonymity of the voter ?

How the voter can check that his vote has been taken into account ? Is there any solution provided to him ?

I need to give my thesis by the end of the month.

Don't hesitate to contact me if needed.

Many thanks in advance

Kind Regards

Michael

Hi Michael:

Please see below in the body of your email.

Thanks,

C. :)

C.L.
IEEE Annual Election

Dear C.,

Many thanks for your reply.

I have further questions relating to the IEEE election.

Which outside firms are managing the election ?
C. -- Survey & Ballot Systems (SBS), Eden Prairie, MN. http://www.surveyandballotsystems.com/. SBS also managed the Circuit and Systems Society and Computer Society election. We send out proposal requests to many election vendors and that's is how we selected SBS. When our three-year contracts ends with SBS, we will again be sending out proposal requests to all the vendors.

I thought it was managed by Intelliscan (firm that I tried to contact to have some information but without any success). My emails are maybe sent as well in the SPAM Box.
C. -- The IEEE annual election uses SBS. Some Societies use Intelliscan and other election firms. There are other firms but I have only worked with SBS since working on the annual election. The annual election is more complex compared to other elections here at the IEEE. Not all election firms are capable of providing the service we are looking for.

Do you know by any chance a contact person there that could help me with my thesis ?
Could you please send them our exchange of mails and see if they can help me ? If not possible, could you please send me the email adress of one person that is working in that firm that could help me.
C. -- I will not be able to give you a contact person. Please feel free send me all your questions and I will do my best to get back to you. I understand that your thesis is due at the end of the month.

In the anwser provided by you, you are describing the full process of the identification but I'd like to know how it is working after that. For example, could you please explain the full voting process ?

Here are some specific questions for the voting process :

I guess the vote is encrypted, but when and how is it done ?
C. -- by encryption, are you referring to the authentication portion? The annual election has two electronic authentication processes. They are:

IEEE Web Account - When members click on the Web Account link, it will take the member back to IEEE. When the authentication is done, an encryption code is sent directly to the election vendor. When the encryption code match, then the vendor's server will automatically let the member access his/her ballot.

Vendor assigned Control Number and E-signature - The vendor's system creates unique login credentials by using the member's eight-digit IEEE #. It's a combination of number and letters.

The annual election process starts a year in advance. For example, I have already started the 2010

election process. Just to give you an idea, here's a high level timeline:

August - Preliminary meeting with IEEE IT team on 2010 election requirements (i.e., Web Account authentication, changes to the ballot datafile, existing/new reports, categories on the ballot, web stats tracking, delivery deadlines, datafiles - QA and live datafile)

September - Submit to IEEE IT the 2010 election requirements

October -
-- Ballot ends on 1 October at 17:00 UTC
-- The IEEE Tellers Committee meets in person on 7 October to certify the annual election results
-- 8 October - unofficial election results become public

November - IEEE Board of Directors meet to accept the election results. Results become official.

December - all known nominated candidates are contacted and requested to provide election material (i.e., photo, biography, history of IEEE volunteer activities, IEEE accomplish statement, statement and by-line/short statement.

15 March 2010 - all nominating units must provide the candidate slates by this date

1 May 2010 - deadline for all candidates to submit all candidate materials

prior to 30 June 2010 - provide election vendor with the slate, biographical booklet information for printing

30 June 2010 - IEEE IT generates the datafiles of all eligible voting members on this date

First week in July 2010 - IEEE IT provides election vendor with the live datafile for creating the election ballots

by 1 August 2010 - Election ballots are mailed to all eligible voting members. Online ballot access will be available on the same day as the ballot mailing.

1 October 2010 at 17:00 UTC - Balloting period ends

Is the server that receives the vote the same than the one that manages the voters list ?
C. -- The IEEE provides the election vendor with the datafile of all eligible voters for them to create the ballots. The vendor receives all the ballots from the members and manages the results. They are two different servers, and neither one has access to the other's server. The IEEE does not have any access to the voting return information (i.e., who voted and voted for what) -- this is for the member's privacy.

In Europe, vote must be secret. Do you guarantee it during your elections ?
C. -- the election voter return information is managed by the election vendor and only the results are provided in a report format. Totals and percentage only, no information on the votes of each member. At the office, we do not know who has voted or not unless the member contacts us to tell us that they need a replacement ballot, can't login or other reasons. We do not have access to the ballot return hosted at the election vendor site. If you have your ballot form, the top part of the ballot is actually detached by the vendor when they are tallying the results. When the paper ballot is received by the vendor, they will scan it in their system and their counter will automatically print a bar code at both the top and bottom portion of the ballot. When the top and bottom is detached, the top part is called the ballot "stub" and it's stored separately. The bottom part is the actual ballot. If we see the bottom portion of the ballot, there is no reference to the member's name and we will not know whose ballot it is if we see it. However, if a ballot is received by the vendor detached, that ballot will be considered an invalid ballot. Only the election vendor can detach the ballot.

How do you manage the voters list ?

C. -- the eligible voting list is created by IEEE. The list is generated for all eligible voting members on 30 June of each year. The 30 June date is not a flexible date. If the member becomes an eligible voter after this date, for example, became a member, renewed a membership, he/she will not receive a ballot.

How are the votes stocked ? How are they decrypted ?
C. -- We do not get to see the ballots that the members return to the vendor or the ballots returned electronically, hosted at the vendor's site. This is all strictly managed by the election vendor at their end. Prior to the actual printing of the ballot, the election vendor stores all the ballot paper in a humidity and temperature controlled room that is locked and accessed is granted to only a selected few at the election vendor's office.

Depending on the election categories that are on the ballot, a permutation is created for each possible ballot combination. For example, this year, we have 17 election categories on the ballot. Using the 17 categories and other factors such as geographic locations, this year we have over 400 different ballots.

How do you guarantee the anonymity of the voter ?
C. -- If the member mails the ballot to the IEEE instead of to the election vendor, the ballot will stay sealed in the envelope and mailed to directly to the election vendor for them to open and tally. If the ballot was mailed to IEEE and a staff opened it by accident, that ballot is considered an invalid ballot and it will still be mailed to the election vendor for tracking as an invalid ballot. The election vendor is not allowed to disclose the voters identify to anyone. They take this very seriously and are hold accountable.

How the voter can check that his vote has been taken into account ? Is there any solution provided to him ?
C. -- All ballots accessed electronically have an option to put in an email address to receive an email confirmation. If the ballot was returned via postal mail, the member can contact the election vendor directly and they can only confirm if a ballot was received or not.

I need to give my thesis by the end of the month.

Don't hesitate to contact me if needed.

Many thanks in advance

Kind Regards

Michael

Annexe 8 : les recommandations du Conseil de l'Europe

Une croix dans la dernière colonne signifie que cette recommandation relève d'un aspect « sécurité ».

Les normes juridiques.

Les principes

- le suffrage universel

1.	L'interface utilisateur du système de vote électronique sera compréhensible et facilement utilisable	
2.	Les éventuelles procédures d'inscription au vote électronique ne constitueront pas un obstacle empêchant l'électeur de participer au vote électronique	
3.	Les systèmes de vote électronique seront, dans toute la mesure du possible, conçus de manière à maximiser les possibilités qu'ils peuvent offrir aux personnes handicapées	
4.	À moins que les modes de vote électronique à distance ne soient universellement accessibles, ils ne constituent qu'un moyen de vote supplémentaire et facultatif	

- le suffrage équitable

5.	Dans toute élection ou référendum, un électeur ne pourra pas déposer plus d'un seul bulletin dans l'urne électronique. Un électeur ne sera autorisé à voter que s'il est établi que son bulletin n'a pas encore été déposé dans l'urne électronique	X
6.	Le système de vote électronique empêchera l'électeur d'exprimer son vote par plusieurs modes de suffrage	X
7.	Tout bulletin déposé dans une urne électronique sera comptabilisé, et tout suffrage exprimé lors d'une élection ou d'un référendum ne sera comptabilisé qu'une seule fois	X
8.	Lorsque des modes de votes électroniques et non électroniques sont utilisés dans un même scrutin, une méthode sûre et fiable permettra d'additionner tous les suffrages et de calculer le résultat correct	X

- le suffrage libre

9.	L'organisation du vote électronique garantira la libre formation et expression de l'opinion de l'électeur et, au besoin, l'exercice personnel du droit de vote	X
10.	La manière dont les électeurs sont guidés durant la procédure de vote électronique ne les amènera pas à voter dans la précipitation ou de manière irréfléchie	
11.	Les électeurs pourront modifier leur choix à n'importe quelle étape de la procédure de vote électronique avant l'enregistrement de leur suffrage, ou même interrompre la procédure, sans que leur choix précédent ne soit enregistré ou que des tiers puissent en prendre connaissance	X
12.	Le système de vote électronique n'autorisera pas les influences destinées à manipuler la volonté de l'électeur pendant le vote	X
13.	Le système de vote électronique offrira à l'électeur un moyen de participer à une	

	élection ou à un référendum sans qu'il ait à exprimer une préférence pour l'une quelconque des opinions de vote, par exemple en déposant un vote blanc	
14.	Le système de vote électronique indiquera clairement à l'électeur que le suffrage a été enregistré avec succès et à quel moment la procédure de vote est terminée	
15.	Le système de vote électronique rendra impossible toute modification d'un suffrage une fois qu'il aura été enregistré	X

- le vote secret

16.	Le vote électronique sera organisé de manière à préserver le secret du vote à toutes les étapes de la procédure et en particulier lors de l'authentification de l'électeur	X
17.	Le système de vote électronique garantira que les suffrages exprimés dans l'urne électronique et le dépouillement sont et resteront anonymes et qu'il est impossible d'établir un lien entre le vote et l'électeur	X
18.	Le système de vote électronique sera conçu de telle manière que le nombre de suffrages attendus dans une urne électronique ne permette pas d'établir un lien entre le résultat et les électeurs individuels	X
19.	Des mesures seront prises pour que les informations requises lors du traitement électronique ne puissent être utilisées pour violer le secret du vote	X

Les garanties de procédures

- la transparence

20.	Les États membres prendront des mesures afin que les électeurs comprennent le système de vote électronique utilisé et aient ainsi confiance en lui	
21.	Des informations sur le fonctionnement du système de vote électronique seront diffusées auprès du public	
22.	Les électeurs se verront offrir la possibilité de s'exercer sur tout nouveau système de vote électronique avant l'enregistrement du suffrage et indépendamment de celui-ci	
23.	La possibilité sera offerte à tous les observateurs, dans les limites fixées par la loi, d'assister à l'élection électronique, de l'observer et de la commenter, y compris au stade de l'établissement des résultats	

- la vérification et la responsabilité

24.	Les composants du système de vote électronique seront divulgués au moins aux autorités électorales compétentes, selon les besoins de la vérification et de l'homologation	X
25.	Avant la mise en service de tout système de vote électronique, et à intervalles réguliers par la suite, en particulier si des changements ont été apportés au système, un organisme indépendant désigné par les autorités électorales compétentes vérifiera que le système de vote électronique fonctionne correctement et que toutes les mesures de sécurité nécessaires ont été prises	X
26.	Le système offrira une possibilité de second dépouillement. D'autres caractéristiques du système de vote électronique qui pourraient peser sur	X

	l'exactitude du résultat seront vérifiables	
27.	Le système de vote électronique n'empêchera pas la nouvelle tenue, partielle ou complète, d'une élection ou d'un référendum	X

- la fiabilité et la sécurité

28.	Les autorités des États membres garantiront la fiabilité et la sécurité du système de vote électronique	X
29.	Toutes les mesures possibles seront prises pour écarter les risques de fraude ou d'intervention non autorisée affectant le système pendant toute la procédure du vote	X
30.	Le système de vote électronique comportera des mesures visant à préserver la disponibilité de ses services durant la procédure de vote électronique. Il résistera en particulier aux dérangements, aux pannes et aux attaques en déni de service	X
31.	Avant toute élection ou référendum électronique, l'autorité électorale compétente vérifiera et établira elle-même que le système de vote électronique est authentique et fonctionne correctement	X
32.	Seules les personnes autorisées par l'autorité électorale auront accès à l'infrastructure centrale, aux serveurs et aux données relatives aux votes. Ces autorisations seront soumises à des règles claires. Les interventions techniques sensibles seront réalisées par des équipes d'au moins deux personnes. La composition de ces équipes changera régulièrement. Dans la mesure du possible, de telles interventions seront réalisées en dehors des périodes électorales	X
33.	Durant la période d'ouverture d'une urne électronique, toute intervention autorisée affectant le système sera réalisée par des équipes d'au moins deux personnes, fera l'objet d'un compte-rendu et sera contrôlée par des représentants de l'autorité électorale compétente et par tout observateur électoral	
34.	Le système de vote électronique préservera la disponibilité et l'intégrité des suffrages. Il assurera également leur confidentialité et les gardera scellés jusqu'au moment du dépouillement. Si les suffrages sont stockés ou transmis hors des environnements contrôles, ils seront cryptés	X
35.	Les votes et les informations relatives aux électeurs resteront scellés aussi longtemps que ces données seront conservées d'une manière qui permette d'établir le lien entre les deux. Les informations d'authentification seront séparées de la décision de l'électeur à une étape prédéfinie de l'élection électronique ou du référendum électronique	X

Les normes opérationnelles.

- la notification

36.	Les règles internes régissant une élection ou un référendum électronique établiront un calendrier clair de toutes les étapes du scrutin ou référendum, aussi bien avant qu'après celui-ci	
37.	La période pendant laquelle un vote électronique pourra être enregistré ne commencera pas avant la notification du scrutin ou du référendum. En particulier	X

	pour ce qui est du vote électronique à distance, cette période sera définie et rendue publique bien avant le début du scrutin	
38.	Bien avant le début du scrutin, les électeurs seront informés dans un langage clair et simple de la manière dont le vote électronique sera organisé et de toutes les démarches qu'ils pourraient avoir à effectuer pour y participer et voter	

- les électeurs

39.	Une liste électorale sera régulièrement mise à jour. L'électeur pourra au moins vérifier les données le concernant qui y figurent et demander des corrections	X
40.	La possibilité de créer une liste électorale électronique et un mécanisme permettant de s'y inscrire en ligne et, le cas échéant, de demander à voter par voie électronique, sera envisagée. Si la participation au vote électronique nécessite une inscription séparée et/ou des démarches supplémentaires de la part de l'électeur, cela pourra se faire par voie électronique et une procédure interactive sera envisagée dans la mesure du possible	X
41.	Dans les cas où la période d'inscription des électeurs et les dates de scrutin coïncident, des dispositions adéquates seront prises pour l'authentification des électeurs	X

- les candidats

42.	La déclaration de candidature en ligne pourra être envisagée	X
43.	Une liste de candidats produite et mise à disposition par voie électronique sera également accessible publiquement par d'autres moyens	X

- le vote

44.	Lorsque le vote électronique à distance se déroule pendant l'ouverture des bureaux de vote, il conviendra tout particulièrement de veiller à ce que le système soit conçu de manière à empêcher tout électeur de voter plusieurs fois	X
45.	Le vote électronique à distance pourra commencer et se terminer avant les heures d'ouverture de tout bureau de vote. Il ne se poursuivra pas après la clôture du scrutin dans les bureaux de vote	X
46.	Pour chaque mode de suffrage électronique, des modalités d'aide et d'assistance concernant les procédures de vote seront établies et mises à la disposition des électeurs. Pour le vote électronique à distance, ces modalités seront également accessibles par des moyens de communication différents et généralement accessibles	
47.	Toutes les options de vote seront présentées de manière égale sur l'appareil utilisé pour l'enregistrement du vote électronique	
48.	Le bulletin électronique servant à enregistrer le suffrage sera exempt de toute information sur les options de vote autre que ce qui est strictement nécessaire à l'expression du suffrage. Le système de vote électronique évitera l'affichage d'autres messages susceptibles d'influencer le choix de l'électeur	
49.	S'il est décidé de permettre l'accès à des informations sur les options de vote à partir du site de vote électronique, ces informations seront présentes de manière égale	

50.	L'attention des électeurs utilisant un système de vote électronique sera explicitement attirée sur le fait que l'élection ou le référendum électronique pour lequel ils vont enregistrer leur vote par des moyens électroniques est une élection ou un référendum réel. S'il s'agit de tests, l'attention des participants sera explicitement attirée sur le fait qu'ils ne sont pas en train de participer à une élection ou un référendum réel, et ceux-ci seront – si les tests sont concomitants aux scrutins – dans le même temps invités à participer à ce scrutin par le(s) mode(s) de suffrage mis à leur disposition à cette fin.	
51.	Le système de vote électronique à distance ne permettra pas à l'électeur d'obtenir une preuve du contenu du suffrage qu'il a enregistré	X
52.	Dans un environnement supervisé, les informations relatives au suffrage disparaîtront de l'affichage vidéo, audio ou tactile utilisé par l'électeur pour exprimer son suffrage dès l'enregistrement de ce dernier.	

- les résultats

53.	Le système de vote électronique ne permettra pas de divulguer le nombre de suffrages exprimés pour les différentes options de vote avant la fermeture de l'urne électronique. Cette information ne sera révélée au public qu'après la clôture de la période du scrutin	X
54.	Le système de vote électronique empêchera que le traitement d'informations relatives aux suffrages exprimés relativement à des sous-ensembles de votants choisis délibérément puisse révéler les décisions individuelles des électeurs	X
55.	Tout décodage nécessaire au dépouillement des voix interviendra dès que possible après la clôture de la période de scrutin	X
56.	Les représentants de l'autorité électorale compétente pourront participer au dépouillement des votes, et les éventuels observateurs pourront observer leur comptabilisation	
57.	Un procès-verbal du dépouillement des votes électroniques sera établi, avec les heures de début et de fin de l'opération ainsi que sur les personnes qui y ont participé	X
58.	En cas d'irrégularité entachant l'intégrité de certains suffrages, ceux-ci sont notés comme tels	X

- l'audit

59.	Le système de vote électronique pourra faire l'objet d'un audit	X
60.	Les conclusions de l'audit seront prises en compte dans la préparation d'élections et de référendums ultérieurs	X

Les exigences techniques.

L'accessibilité

61.	Des mesures seront prises pour garantir que les logiciels et les services concernés puissent être utilisés par tous les électeurs et, si nécessaire, pour fournir un accès à d'autres modes de vote	

62.	Les utilisateurs seront impliqués dans la conception des systèmes de vote électronique, en particulier pour identifier les contraintes et tester la facilité d'utilisation à chaque étape majeure du processus d'élaboration	
63.	Les utilisateurs se verront offrir, si la demande en est faite et que la possibilité existe, des fonctions complémentaires telles que des interfaces spéciales ou d'autres ressources équivalentes, comme une assistance personnelle. Les fonctions d'utilisateur seront, autant que possible, conformes aux directives de l'Initiative d'accès au Web (Web Accessibility Initiative – WAI)	
64.	Dans la conception de nouveaux produits, il conviendra de veiller à leur compatibilité avec les produits existants, y compris ceux utilisant des technologies d'assistance aux personnes handicapées	
65.	La présentation des options de vote sera optimisée pour l'électeur	

L'interopérabilité

66.	Des normes ouvertes seront utilisées pour garantir l'interopérabilité des divers éléments techniques ou services d'origines éventuellement différentes d'un même système de vote électronique	
67.	Actuellement, l'EML (Election Markup Language) est une telle norme ouverte et, afin de garantir l'interopérabilité, l'EML sera utilisée autant que possible dans les applications destinées aux élections et référendums électroniques. Le délai du passage des procédures de votes électroniques actuelles à l'EML est laissé à l'appréciation des États membres. La norme EML en vigueur lors de l'adoption de cette recommandation et la documentation explicative sont disponibles sur le site du Conseil de l'Europe	
68.	Les besoins spécifiques en matière de données électorales ou référendaires seront gérés par un processus d'adaptation aux conditions locales. Cela permettra d'étendre ou de restreindre les informations à fournir, tout en préservant leur compatibilité avec la version générique de l'EML. La procédure recommandée est l'utilisation d'un langage de schéma structuré et de modélisation	

Le fonctionnement des systèmes (pour l'infrastructure centrale et les clients dans des environnements contrôlés)

69.	Les autorités électorales compétentes publieront une liste officielle des logiciels utilisés durant un vote ou un référendum électronique. Les États membres peuvent, pour des raisons de sécurité, omettre les logiciels de sécurité de cette liste. Celle-ci spécifiera au minimum les logiciels utilisés, leur version et leur date d'installation, et fournira une brève description. Une procédure sera établie pour l'installation régulière des mises à jour et des corrections des logiciels de protection concernés. L'état de protection des équipements de vote pourra être vérifié à tout moment.	X
70.	Les personnes en charge du fonctionnement des équipements définiront une procédure de secours. Tout système de remplacement répondra aux mêmes normes et exigences que le système original.	X

71.	Des mesures de secours suffisantes seront mises en place et disponibles en permanence afin d'assurer un déroulement sans heurt du scrutin. Le personnel concerné sera prêt à intervenir rapidement selon une procédure établie par les autorités électorales compétentes.	X
72.	Les responsables de l'équipement disposeront de procédures pour garantir que, durant le déroulement du scrutin, les équipements de vote et leur utilisation satisfont aux exigences requises. Des protocoles de contrôle seront régulièrement fournis aux services de secours	X
73.	Avant chaque scrutin ou référendum, l'équipement sera vérifié et approuvé conformément à un protocole établi par les autorités électorales compétentes. L'équipement sera vérifié afin de garantir sa conformité aux spécifications techniques. Les conclusions seront soumises aux autorités électorales compétentes	X
74.	Toute opération technique sera soumise à une procédure officielle de contrôle. Tout changement substantiel sur un équipement clé sera notifié.	X
75.	Les équipements clés du vote ou référendum électronique seront situés dans une zone protégée, gardée en permanence contre des interférences de toutes sortes et de toutes personnes pendant la période du scrutin ou du référendum. Un plan de prévention des risques physiques sera mis en place pendant la période du scrutin ou du référendum. De plus, toutes les données conservées après la période du scrutin ou du référendum le seront en lieu sûr	X
76.	En cas d'incident susceptible d'affecter l'intégrité du système, les personnes chargées du fonctionnement de l'équipement en informeront automatiquement les autorités électorales compétentes, qui prendront les mesures nécessaires pour en atténuer les effets. Le niveau d'incident à signaler sera spécifié à l'avance par les autorités électorales.	X

La sécurité

- les exigences générales (périodes préélectorale, du scrutin et postélectorale)

77.	Des mesures techniques et organisationnelles seront prises pour s'assurer qu'aucune donnée ne sera définitivement perdue en cas de panne ou de défaut affectant le système de vote électronique.	X
78.	Le système de vote électronique préservera la vie privée des personnes. La confidentialité des listes électorales enregistrées ou communiquées par le système sera assurée.	X
79.	Le système de vote électronique vérifiera régulièrement la conformité aux spécifications techniques du fonctionnement de ses éléments et la disponibilité de ses services.	X
80.	Le système de vote électronique restreindra l'accès à ses services, en fonction de l'identité de l'utilisateur ou de son rôle, aux services explicitement ouverts à cet utilisateur ou à ce rôle. L'identité de l'utilisateur sera établie avant toute action.	X
81.	Le système de vote électronique ou ses éléments protègeront les données d'authentification de manière à empêcher des entités non autorisées de détourner, d'intercepter, de modifier ou de prendre connaissance de toute autre manière de tout ou partie de ces données. Dans des environnements non	X

	contrôlés, il est recommandé de recourir à une authentification fondée sur la cryptographie.	
82.	L'identification des électeurs et des candidats sera assurée d'une manière qui permette de les distinguer sans le moindre doute de toute autre personne (identification exclusive)	X
83.	Le système de vote générera des données d'observation assez détaillées et fiables pour permettre l'observation du scrutin. Il sera possible de déterminer de manière fiable la date et l'heure à laquelle un événement a généré des données d'observation. L'authenticité, la disponibilité et l'intégrité des données d'observation seront assurées.	X
84.	Le système de vote électronique sera doté d'horloges synchronisées fiables. La précision de ce système d'horodatage sera suffisante pour gérer l'enregistrement de la date et l'heure des relevés d'audit et des données d'observation, ainsi que les limites des délais d'inscription, de désignation, de vote ou de dépouillement.	X
85.	Les autorités électorales assumeront la responsabilité générale du respect de ces exigences de sécurité, qui seront contrôlées par des organismes indépendants.	X

- les exigences en période préélectorale (et pour les données transmises en période de scrutin)

86.	L'authenticité, la disponibilité et l'intégrité des listes électorales et des listes de candidats seront préservées. L'origine des données sera authentifiée. Les dispositions relatives à la protection des données seront respectées.	X
87.	Il sera possible d'établir si la désignation des candidats et, le cas échéant, la décision du candidat et/ou de l'autorité électorale compétente d'accepter une désignation sont intervenues dans les délais prescrits.	X
88.	Il sera possible d'établir si l'inscription des électeurs est intervenue dans les délais prescrits.	X

- les exigences pendant la période du scrutin (et pour les données transmises à la période postélectorale)

89.	L'intégrité des données communiquées à partir de la période préélectorale (par exemple les listes électorales et les listes de candidats) sera assurée. L'origine des données sera authentifiée.	X
90.	On garantira que le système de vote électronique présente un bulletin authentique à l'électeur. En cas de vote électronique à distance, l'électeur sera informé des moyens de vérifier que la connexion est établie avec le serveur authentique et qu'un bulletin authentique lui est présenté.	X
91.	Il sera possible d'établir qu'un suffrage a été exprimé dans les délais prescrits.	X
92.	Des mesures suffisantes seront prises pour assurer la protection des systèmes utilisés par les électeurs pour exprimer leur suffrage contre des influences pouvant modifier leur décision.	X
93.	Les informations résiduelles qui renferment la décision de l'électeur ou l'image d'écran où s'affiche son choix seront détruites dès que le suffrage est exprimé. En cas de vote électronique à distance, l'électeur sera informé de la procédure à suivre pour effacer, si possible, les traces du suffrage exprimé de l'appareil utilisé	X

	pour enregistrer son suffrage.	
94.	Le système de vote électronique vérifiera en premier lieu que l'utilisateur qui essaie de voter est habilité à le faire. Le système authentifiera l'électeur et s'assurera que seul le nombre approprié de suffrages par électeur sera enregistré et stocké dans l'urne électronique.	X
95.	Le système de vote électronique garantira que la décision de l'électeur sera représentée avec exactitude dans le suffrage exprimé et que le vote scellé parviendra à l'urne électronique.	X
96.	À l'issue de la période du scrutin électronique, aucun électeur n'aura accès au système de vote électronique. L'acceptation des suffrages électroniques dans l'urne électronique se poursuivra toutefois pendant un délai acceptable pour tenir compte des éventuels retards de transmission des messages au travers des différents modes de vote électronique.	X

- les exigences pendant la période postélectorale

97.	L'intégrité des données communiquées pendant la période du scrutin (par exemple votes, inscription des électeurs, liste des candidats) sera préservée. L'origine des données sera authentifiée.	X
98.	Le dépouillement décomptera les voix avec précision. Il sera reproductible.	X
99.	Le système de vote électronique assurera, aussi longtemps que nécessaire, la disponibilité et l'intégrité des urnes électroniques et du résultat du dépouillement.	X

L'audit

- général

100.	Le système d'audit sera conçu et implanté comme une partie intégrante du système de vote électronique. Des fonctions d'audit existeront à différents niveaux du système : logique, application et technique.	X
101.	Un audit complet d'un système de vote électronique inclura l'enregistrement, la fourniture des fonctions de contrôle et celle des fonctions de vérification. C'est pourquoi des systèmes d'audit possédant les caractéristiques exposées précédemment seront utilisés pour satisfaire à ces exigences.	X

- l'enregistrement

102.	Le système d'audit sera ouvert et complet, et signalera activement les problèmes et menaces potentiels.	X
103.	Le système d'audit enregistrera les dates et les heures, les événements et les actions, y compris I. toutes les informations relatives au scrutin, y compris le nombre d'électeurs habilités, le nombre de suffrages exprimés, le nombre de votes déclarés invalides, les dépouillements, etc. ; II. toute attaque contre le système de vote électronique et ses infrastructures de communication ; III. les pannes du système, ses défaillances et les autres menaces contre le système.	X

- le contrôle

104.	Un système d'audit permettra de surveiller l'élection ou le référendum et de vérifier la conformité des résultats et des procédures électorales aux dispositions légales pertinentes.	X
105.	Les informations de l'audit ne seront pas divulguées à des personnes non autorisées.	X
106.	Le système d'audit préservera constamment l'anonymat des électeurs.	X

- la vérification

107.	Le système d'audit permettra de faire le contrôle croisé et la vérification du bon fonctionnement du système de vote électronique et de l'exactitude du résultat, de détecter les fraudes des électeurs et de fournir la preuve que tous les suffrages comptabilisés sont légitimes et que tous les votes authentiques sont comptabilisés.	X
108.	Un audit permettra de vérifier qu'un scrutin ou un référendum électronique s'est déroulé conformément aux dispositions juridiques applicables, l'objectif étant d'établir que les résultats représentent les suffrages authentiques de manière exacte.	X

- divers

109.	Le système d'audit sera protégé contre les attaques susceptibles de corrompre, d'altérer ou de détruire ses propres données.	X
110.	Les États membres prendront les mesures nécessaires pour garantir la confidentialité de toute information obtenue par toute personne participant à l'audit.	X

L'homologation

111.	Les États membres sont invités à mettre en place des procédures d'homologation permettant de tester tout élément informatique et de vérifier sa conformité aux exigences techniques décrites dans cette recommandation.	X
112.	Soucieux d'améliorer la coopération internationale et d'éviter les doubles emplois, les États membres envisageront de faire adhérer leurs organismes respectifs qui ne l'auraient pas encore fait aux accords internationaux pertinents de reconnaissance mutuelle tels que la Coopération européenne pour l'accréditation (European Cooperation for Accreditation-EA), la Coopération internationale sur l'agrément des laboratoires d'essais (International Laboratory Accreditation Cooperation-ILAC), le Forum international de l'accréditation (International Accreditation Forum-IAF) et les autres organismes similaires.	