MASTER IN COMPUTER SCIENCE

Etude des systèmes de vote électronique: E-vote et I-vote

Henrioulle, Bernard

Award date:
2001

FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX, NAMUR

INSTITUT D'INFORMATIQUE

RUE GRANDGAGNAGE, 21, B-5000 NAMUR (BELGIUM)

ETUDE DES SYSTEMES DE VOTE ELECTRONIQUE

E-Vote & I-Vote

Bernard HENRIOULLE

Mémoire présenté en vue de l'obtention du grade de
Licencié en Informatique

Année Académique 2000 - 2001

Résumé - Summary

Ce mémoire a pour but d'établir une liste des règles et contraintes à appliquer à tous développements de systèmes d'élection électronique utilisant ou non une connexion à un réseau.
Le résultat insistera sur l'importance de la confiance de l'électeur pour le système d'élection et sur le respect des règles d'unicité, d'intégrité et de confidentialité.
Nous présenterons aussi des techniques de sécurisation des données et de chiffrement des informations.
Enfin, il sera possible d'envisager différents types d'implémentations suivant que le système d'élection électronique utilise ou non une connexion à un réseau.
Nous effectuerons une étude comparative ainsi que la critique, notamment sur la sécurité, pour les différents systèmes.
Des solutions et des produits informatiques permettant le vote électronique lors d'élections officielles seront également présentés.
Nous étudierons pour les élections électroniques sans connexion à un réseau, le système d'élection automatisé "belge" et le système français de la "valise à voter".
Il y aura également la présentation des tests d'implémentations "américains" pour l'organisation d'élections électroniques avec une connexion au réseau Internet et les projets européens pour les années futures.
En fin de mémoire, nous fournirons une grille d'analyse et de comparaison pour les différents exemples d'implémentations.

The goal of this thesis is to establish a list of rules and constraints to be taken into account when an electronic voting system is considered. This system can either be connected to a network or self-standing.
The conclusion drawn from this thesis will take into consideration the feelings of the individual voter have towards the respect of continuity, integrity and confidentiality.
The study will elaborate on techniques relating to the security of the data and the encrypting of the information.
Finally several methods of implementation will be reviewed taken into account the connectivity to a network or the stand-alone character. A comparative analysis of the different systems will be performed taking into account security issues. The results are presented in a grid format at the end of the thesis.
This study will also review the different solutions commercially available dealing with the electronic voting system.
A review of the already implemented system will be presented and divided into two categories. The first one will review the stand-alone systems used in Belgium (automatic voting system), the second one used in France called the voting satchel.
The second part of the study will deal with the solutions connected to a network being tested at this time in the United States of America as well as solutions using Internet.

Avant-propos

Ce mémoire de fin d'études a représenté une charge de travail importante car il a demandé de nombreuses recherches et collectes de données. Grâce aux interventions et aux informations de certaines personnes, ce travail a pu être finalisé.

Je remercie vivement les personnes suivantes :

M. L. VANNESTE, Directeur général, Direction générale de la législation et des institutions nationales. Direction des Elections et de la Population.

M. J. DE BEENHOUWER, Ministère de l'intérieur, Service du Fonctionnaire de l'information.

Madame Dany REMACLE, consultante informatique.

Mademoiselle Dominique TESTA, informaticienne.

De plus, je suis très reconnaissant pour le soutient et l'encouragement apporté par Monsieur RAMAEKERS, professeur et promoteur aux F.U.N.D.P.

Merci également aux anonymes qui ont répondu à mes demandes de renseignements ou à mes appels téléphoniques dans le cadre de mes recherches.

Je terminerai en saluant particulièrement le mérite de ma famille et de mes amis proches pour avoir supporté et encouragé l'étudiant que j'étais redevenu pour cette licence à horaire décalé.
Aussi bien dans les moments d'angoisses, que dans ceux de doutes et de stress, jamais leur soutient n'a été pris en défaut.

Table des matières

Introduction

Où en sommes-nous et où allons-nous dans la conception et l'utilisation des systèmes de votes électroniques pour l'organisation d'élections officielles ?

Pour y répondre, ce mémoire regroupe, synthétise et analyse un ensemble d'études et de rapports sur le vote électronique.

Nous allons apporter un ensemble de règles et de contraintes qui tout en restant neutres au niveau technologique, sont applicables aussi bien à des systèmes d'élections classiques "papier", qu'à des élections électroniques (E-Vote) ou par réseaux (I-Vote).

Lorsque nous identifions un système de vote électronique, il est important d'opérer une distinction dès le départ entre les systèmes qui utilisent des solutions informatiques sans connexion à un réseau et qui seront identifiés comme "Electronic-Voting System" ou *E-Vote*, et les systèmes qui utilisent des solutions informatiques mais avec une connexion à un réseau ou à Internet et qui seront identifiés comme "Internet-Voting System" ou *I-Vote*.

De plus, les règles et contraintes qui seront définies dans ce mémoire, répondront aux obligations particulières à respecter par tous systèmes d'élections officielles.

Les autres types d'élections, identifiés comme privées, sont moins strictes ou utilisent des règles propres en rapport avec le secteur d'activité pour lequel l'élection est organisée. Elles pourraient éventuellement respecter les règles ici exposées, mais celles-ci seront en général trop ardues pour ce type d'élection.

Le mémoire présentera également des implémentations de différents systèmes de vote, aussi bien *E-Vote* que *I-Vote*. Chaque système sera présenté et ensuite analysé sur base des règles et contraintes définies au début du travail. Les exemples qui sont exposés proviennent d'implémentations ou d'expérimentations belges, européennes et américaines.

Enfin, la grille d'analyse qui aura été développée, pourra également par la suite servir d'outil de référence pour la critique de tout système d'élection électronique qui serait proposé et ceci indépendamment de toutes considérations politiques.

Chapitres

1 Définition de règles et contraintes pour les systèmes d'élections électroniques.

1.1 Définition d'un système d'élection

En vue de définir les exigences à appliquer pour la création de systèmes de votes électroniques, nous nous basons sur les organisations d'élections officielles classiques dénommées "Election avec bulletin de vote en papier".

Qu'est ce qu'un système d'élection classique ?

Rappelons qu'une élection est un choix effectué par la voie des suffrages. Le suffrage dit "universel direct", est un système par lequel le corps électoral est constitué par tous les citoyens qui votent directement pour les candidats à élire.
Pour une élection au suffrage universel, des électeurs et des bulletins de vote avec la liste des candidats sont nécessaires.
Pour avoir droit au vote, l'électeur devra être identifié et authentifié. De plus, il ne pourra voter qu'une seule fois.
L'électeur exprimera son choix secrètement et anonymement sur un bulletin de vote qu'il placera dans une urne.
Après la clôture de la période d'élection, l'urne sera dépouillée et les votes seront comptabilisés afin d'éditer le résultat des candidats élus.

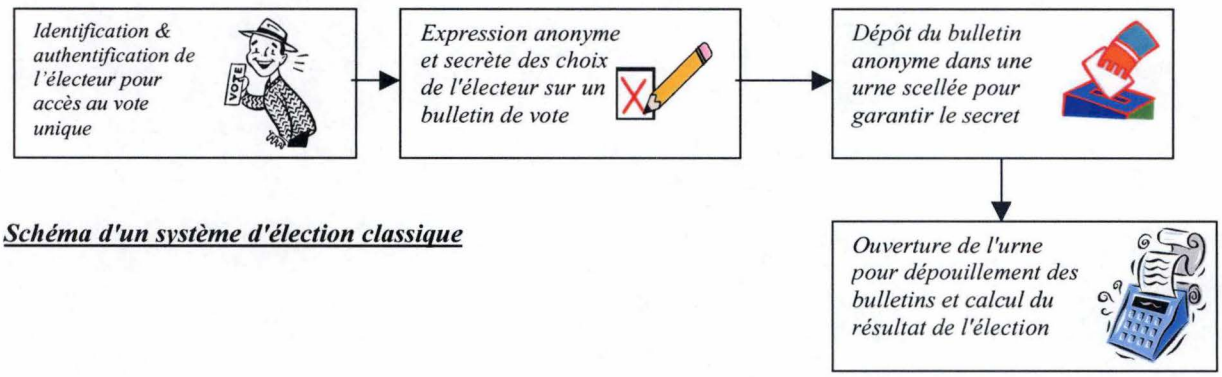


Schéma d'un système d'élection classique

De tels systèmes d'élections dit "classiques", sont depuis très longtemps en fonction et peuvent être considérés comme correct si l'ensemble des intervenants humains sont tous de confiance et effectuent leur tâche sans erreur.

Si tel est le cas, nous avons alors un système d'élection répondant à différents critères qui sont les bases de tous systèmes d'élections officielles, c'est-à-dire :

- *anonyme* : il est impossible de connaître l'identité de l'électeur à partir d'un vote afin d'éviter les collusions et les contraintes;
- *secret* : le vote de chaque électeur est inconnu et confidentiel;
- *correct* : tous les votes exprimés sont interprétés et comptabilisés correctement;
- *honnête*: personne ne peut voter plus d'une fois ou changer le vote d'une autre;
- *complet* : tous les électeurs doivent voter ou justifier leur absence;

Au départ de la procédure d'élection, les électeurs sont identifiés mais nous ne pouvons connaître la valeur de leurs votes et si nous connaissons un vote, par exemple au moment du dépouillement, nous ne pouvons pas le rattacher à l'électeur.

Après la clôture de l'élection, tous les identifiants des électeurs et tous les choix des votes peuvent être publiquement connus, mais la relation entre électeur et vote est impossible et inconnue.

La validité des systèmes "classiques" repose donc uniquement sur des valeurs humaines avec le respect de procédures strictes et l'exécution correcte des tâches prévues.
Comme "*Tout est humain, surtout les faiblesses, les erreurs, les lâchetés*" ***[Driss Chraïbi]***, dans la réalité de tels systèmes sont sensibles et pas toujours parfaitement utilisés.

L'utilité du développement d'un système d'élection utilisant la technologie informatique, est d'être plus sécurisant et aussi correcte qu'un système d'élection classique reposant exclusivement sur des intervenants humains.

1.2 Confiance objective et vérification de l'information.

Il serait trop simpliste de qualifier, par défaut, une méthode d'élection utilisant la technologie informatique, plus sécurisant et aussi correcte qu'un système d'élection classique reposant exclusivement sur des intervenants humains.

Nous devons alors introduire le concept de "Confiance dans l'information et l'informatique" afin de fournir différentes preuves attestant de la validité des modèless d'élections utilisant cette technologie ***[The Bell]***.

Il faut que les preuves fournies puissent être évaluées objectivement et notamment la confiance en la validité de l'information qui circule dans l'architecture informatique mise en place.

Une solution pour les architectures d'élections électroniques informatisées repose sur le principe d'utilisation de canaux de communications multiples et indépendants entre les différents composants humains ou machines afin de fournir des preuves de confiance et des vérifications de l'information.

1.2.1 Vérification par le système d'élection

Par exemple, comment un système d'élection électronique peut prouver que le vote reçu dans l'urne est le même que celui "noirci" sur le bulletin de vote par l'électeur ?

Le problème est, que l'électeur n'a pas la possibilité de savoir et de contrôler si le vote qu'il a exprimé est arrivé dans l'urne via le "Canal de Communication" avec la même valeur qu'à l'origine. La distance de ce "Canal" n'a pas réellement d'importance ***[The Bell]***.

Pour solutionner ce problème, certaines architectures de systèmes d'élections électroniques proposent une impression d'un ticket preuve sur lequel l'électeur peut vérifier si le vote est identique à celui qu'il a exprimé sur un terminal de vote informatisé.
L'électeur doit ensuite placer son ticket dans une urne "classique" au bureau de vote tandis que son vote électronique est transféré, par un autre canal de communication, dans une urne électronique.

Cette architecture propose une solution utilisant deux canaux de communications indépendants pour le bulletin de vote; un via le vote électronique, et un autre via l'impression du bulletin papier et le placement de celui-ci dans une urne traditionnelle.

Ici, nous sommes ici en présence d'une solution utilisant N canaux indépendants avec N=2.

Malgré la redondance de canaux, cette solution n'apporte pas de "confiance en l'information" objective en cas de problème.

En effet, si une différence est observée entre les résultats fournis par le vote électronique et les résultats des votes sur ticket papier, il n'y aura pas de solution au travers du système ainsi définit. Il faudra donc de manière subjective ou par une règle établie donner la préférence à un des deux résultats.

En fait, les modèles utilisant un seul canal de communication, reposent sur une confiance absolue dans le bon fonctionnement des différents acteurs du système (humain ou matériel), mais n'offrent aucune solution objective de vérification.

Le fait d'ajouter un deuxième canal de communication indépendant permet au système d'identifier et déterminer une erreur en cas de différence entre les deux canaux, mais il ne permet pas de solutionner le problème.

Il faut donc multiplier le nombre de canaux afin de trouver des solutions logiquement prouvables en cas de problèmes de communication entre les différents composants et ceci dans les relations aussi bien de machine à machine, d'humain à machine et également d'humain à humain.

C'est pourquoi l'architecture qui consiste à ajouter une copie papier du vote à une organisation d'élection électronique n'est pas efficace car elle n'apporte pas de solution objective en cas de différences dans les résultats.

La décision du choix de la solution correcte devra être prise à priori et en dehors du système.
De plus, nous augmentons les possibilités de fraudes pour faire annuler ou modifier les élections.

Nous pouvons confirmer qu'il est donc nécessaire que les modèles reposent sur la définition de canaux de communication indépendants d'un nombre N supérieur à 2 pour toutes les connexions entre les différents acteurs afin de fournir des preuves de validités de l'information et ainsi éviter un système reposant sur une confiance unique et absolue (N=1).

Ainsi, plus il existe de canaux indépendants pour la vérification de l'information, plus grande sera la confiance dans le modèle d'organisation.

Mais supposons un système avec un terminal sur lequel l'électeur entre son choix de vote et qu'un élément perturbateur et interne au terminal change la valeur du vote exprimé avant de l'envoyer sous forme électronique vers l'urne et ceci au travers de N canaux différents. D

Dans un tel cas, qu'est-ce qui change dans la confiance au système si N = 1 ou 2 ou 500 ?

Ici, absolument rien. Donc N peut rester 1 pour le canal de communication du bulletin car, dans les autres solutions avec N= 2 ou 500, les canaux ne sont pas indépendantes.
Elles ne le sont pas car elles transmettent toutes une même copie du vote qui a été modifiée sur le terminal avant l'envoi sur les canaux.

Ici la multiplication des canaux n'apporte pas de solution de confiance supplémentaire dans la validité du vote, mais apporte seulement plus de confiance dans la validité de la connexion entre le terminal et l'urne.
En effet avec un nombre de canaux N d'une certaine valeur, nous pourrons seulement vérifier que l'urne reçoit bien l'information envoyée par le terminal, mais qui a été éventuellement corrompue avant l'envoi.

Nous avons donc besoin de systèmes comprenant de multiples canaux de communication réellement indépendants pour vérifier la confiance dans le vote (lien d'humain à machine), la transmission de données (lien de machine à machine) et les audits de contrôle (lien d'humain à humain).

Cette demande de redondance de canaux indépendants sera aussi bien mise en place pour les transactions électroniques que pour les transactions manuelles.

Le contrôle des différents canaux, apportera la confiance pour chaque point composant le chemin de l'information, du début à la fin d'une élection.

Un canal de communication peut aussi transporter l'information par référence et pas uniquement par valeur afin de simplifier et alléger les connections.

1.2.2 Vérification par l'électeur

Il sera alors demandé à toutes les organisations de vote électronique de permettre à l'électeur de vérifier certaines informations telles que :

- la présence ou l'absence de son vote dans l'urne;
- la validité de son vote.

Cette particularité de vérifications indirectes et individuelles par les électeurs permet d'augmenter la confiance dans le système adopté.

"Solution de confiance mais vérifiable" ***[Dictson & Ray 1]*** sera la devise de tous développements de système d'élections électroniques.

Il est important de noter que même si un nombre limité d'électeurs souhaitent exécuter une procédure de contrôle, cette possibilité pourra être dissuasive pour d'éventuelles malversations car les fraudeurs n'auront pas les moyens de savoir quand et quel électeur effectuera une vérification.

Une autre caractéristique d'un bon système de vérification de vote est que seule la personne à qui on prouve le vote est l'électeur même.
De plus seule la réception du vote dans l'urne sera prouvée, mais en aucun cas le contenu du bulletin et les choix de l'électeur.

Si cette preuve peut être fournie à une autre personne ou contenir l'information sur le vote, alors il y existe des risques de collusion ou de contrainte pour l'électeur.

Les mesures de protection contre la divulgation de la preuve de vote sont donc très importantes, notamment dans le cas de l'utilisation de canaux de communications multiples où l'information est dupliquée et passe par différents chemins du réseau de communication.

1.2.3 La confiance de l'électeur

Une des questions à poser pour toutes les architectures de système d'élection électronique est : "Avons-nous confiance et pourquoi ?" ***[Dictson & Ray 2]***

De nos jours, des systèmes informatiques ou électroniques sont utilisés par exemple dans l'aviation commerciale ou militaire pour l'assistance au pilotage.
Et pourtant le grand public n'est pas inquiet de la possibilité qu'un groupe terroriste introduise un virus dans un tel système pour par exemple, provoquer le crash aérien d'un avion civil.

Pourquoi cette crainte n'existe-t-elle pas comme pour les systèmes d'élections électroniques ?

Simplement parce que le public est convaincu que l'électronique ou l'informatique utilisée a été conçue avec des redondances de matériel, de logiciel et des contrôles à plusieurs niveaux des installations.
Par exemple, les systèmes de navigation dans l'aviation utilisent trois capteurs dont au moins deux doivent donner un résultat identique et qui lui-même sera vérifié par un système de positionnement GPS (solution à N canaux indépendants d'informations).

Donc, le public peut acquérir la confiance dans les organisations d'élections électroniques si nous lui apportons des informations pour lui permettre une certaine compréhension et une appréhension suffisamment logique du système et de l'architecture de sécurité qui aura été installée.

Il faut donc informer le grand public des solutions choisies afin de protéger les enregistrements et communications électroniques des attaques des fraudeurs, aussi bien par des moyens de contrôle physique d'accès que par l'utilisation de protocole de sécurité ou de chiffrement.

L'électeur est suffisamment conscient que tout système d'élection traditionnelle peut être faussé si un nombre suffisant de personnes qui organisent l'élection sont corrompues.
Néanmoins le fait qu'une quantité énorme de bulletins papiers soient comptabilisée et vérifiée, représente un obstacle physique à une fraude ou subversion facile.

Par contre l'électeur est souvent convaincu qu'une fraude dans les systèmes et réseaux informatiques pourrait modifier des millions d'enregistrements de votes électroniques en très peu de temps. Il fait donc face à la crainte d'une subversion massive et rapide qu'il considère difficilement inévitable.

Naturellement, une des alternatives pour réduire cette peur est l'éducation de l'électeur en l'informant simplement sur les techniques de chiffrement et de sécurité informatique.

Pour l'architecture informatique, il faut également utiliser au maximum la redondance des canaux de confiance dans le système de communication afin de rendre impossible l'ajout ou la suppression de votes qui pourraient compromettre la validité des élections et faire perdre la confiance des électeurs.
Pour tout fraudeur, il sera difficile d'attaquer l'ensemble des canaux simultanément et si cela était possible, ce serait dû au fait que les canaux n'étaient pas indépendants tel que prévu dans les contraintes.

Le principe de redondance des canaux de communication indépendants s'applique donc à un principe général d'élection tout en restant valide pour n'importe quelle implémentation physique du vote, que ce soit sur papier, gravé sur un CD-ROM, en touchant un écran tactile sur une console de vote ou encore en envoyant un message électronique sur un réseau.

Pour conclure sur la confiance dans un système, il est intéressant de construire et fournir une liste d'exigences et de contraintes qui est applicable à n'importe quel système de vote.
C'est pourquoi, le principal objectif de cette liste est d'être complète et surtout de donner des exigences indépendantes les unes des autres autant que possible sans sacrifier la consistance.

Il est compréhensif, qu'affirmer que la règle qui demande qu'une élection soit "complète" est trop évasive et que cette règle ne pourra jamais être totalement traduite en une exigence car il existe une trop grande diversité de types et règlements d'élections.

C'est la raison pour laquelle la liste des règles et contraintes doit être limitée.
L'augmentation de contraintes risque de faire décroître la consistance en générale.

Cela n'empêche pas la possibilité d'ajouter ou de supprimer certaines règles et contraintes suivant l'application ou le type d'élection, notamment pour les différences entre les élections officielles et privées.

1.3 Authentification et unicité

Toute organisation d'élection doit permettre l'authentification de l'électeur afin de pouvoir vérifier ***[Jones]*** :

- le droit au vote de l'électeur;
- l'unicité du vote.

Les moyens d'identifications existeront en fonction du type d'implémentation du système d'élection avec par exemple :

- pointage par un organisateur des élections dans une liste de l'électeur lors de sa présentation dans un bureau de vote après présentation de sa carte d'identité;
- identification sur un terminal de vote par l'électeur même avec l'introduction de son numéro d'identification unique et d'un code secret.

Chaque architecture devra rendre impossible la reconnaissance de l'identifiant ou le nom de l'électeur à partir d'un vote et vice versa.

Il sera également impossible à une personne de se faire identifier comme étant une autre et donc de voter à sa place, sauf en cas d'acceptation des procurations de vote et ceci après l'application de règles de contrôle strictes.

L'organisation devra autoriser l'électeur à voter une seule fois ou du moins ne plus permettre le vote une fois que celui-ci est accepté et comptabilisé par le système.

Les techniques informatiques de certification et de signature électronique seront d'application dans les étapes d'identifications des électeurs par des systèmes automatisés.

D'autres techniques telles que l'identification sur base de particularités humaines uniques (Biométrie) ou l'utilisation de carte à puce électronique (Smartcards) seront envisagées suivant les évolutions futures des techniques ici exposées. ***[Bio & Secu]***

Le chapitre sur la sécurisation des données présentera plus en détail les différentes techniques citées.

1.4 Intégrité et confidentialité

Il est très important de rappeler que l'intégrité de tout système de vote est le fondement de la confiance en celui-ci ***[Jones]***.

Il faut donc développer les outils et méthodes de contrôle interne et externe afin d'empêcher toutes modifications ou suppressions de vote pour garder le système intègre et correct.

Des méthodes d'audits seront développées pour contrôler et certifier la validité des résultats des élections.

La sécurité du système sera développée contre les attaques électroniques telles que virus, Denial of Service, Spoofing, Changement du code,.... qui pourraient détruire, détourner, modifier et consulter les informations. ***[Guill.net]***

Enfin, il est important de sauvegarder la confidentialité et le secret du vote.

Cette préservation du secret est un des fondements de la confiance en la validité des élections.

Ne jamais rattacher un vote à son électeur tout en voulant assurer l'intégrité et la validité d'une élection n'est pas chose facile.

Cette confidentialité est totale dans les organisations classiques d'élection papier avec l'obligation de voter seul dans un isoloir après l'identification de l'électeur par un responsable du bureau de vote.

Ainsi donc, toute autre solution, totalement ou partiellement informatisée, ne pourra offrir moins de confiance dans la confidentialité du vote.

La confidentialité, le secret et l'intimité du vote d'un électeur sont les exigences les plus importantes à garantir par les systèmes de votes.

La solidité du secret de l'électeur peut être protégée à différents niveaux de la procédure d'élection, mais peut également subir différents types d'attaques.

Dans le tableau suivant, nous analysons les différents types de protection du secret en partant du "moins solide" au "plus stable", et nous pouvons pour chacun nommer le principe de protection et les types d'attaques possibles. ***[The Bell]***

Solidité	Type de protection du secret	Principe de protection	Types d'attaques
-	Règlement politique et procédures strictes à suivre.	Respect des règles de sécurités et des procédures établies pour l'échange d'informations.	Non suivi des règles Connivence d'acteurs Ordre des autorités de casser le secret
+/-	Protection informatique.	Code de programme informatique correct et implémentation dans du matériel certifié et vérifié.	Casser ou modifier le code Obtention des clefs Connivence des programmeurs Ordre des autorités de casser le secret
+	Théorie de protection de l'information.	Relation improuvable entre vote et électeur par chiffrement non traduisible	Obtention du secret Connivence des programmeurs Ordre des autorités de casser le secret
++	Sécurité totale.	Aucune relation possible	Aucunes

Le modèle de type "Sécurité totale" est utilisé actuellement par les élections de type classique avec bulletin de vote papier et urne de vote traditionnelle.
En effet, il sera impossible de relier l'identité de l'électeur aux votes exprimés ni en cas de connivence ou même d'instructions des autorités du pays pour casser le secret.

Certaines solutions de vote informatisé affirment pouvoir offrir des garanties identiques, notamment l'architecture proposée par la société américaine SafeVote : ***[SafeVote]***

- en ne révélant jamais les informations privées d'identités des électeurs au système de vote et ceci sous n'importe quelle forme;
- en créant une structure de contrôle anonyme des votes électroniques par l'utilisation d'une certification des votes et la technique de chiffrement homomorphique.

L'architecture du système de la société SafeVote offre une solution mathématique pour le contrôle de la validité des données sans jamais permettre la mise en relation avec l'identité de l'électeur.

Nous présenterons cette solution lors de l'analyse et la comparaison de différentes implémentations ou expérimentations d'organisations de votes électroniques.

1.5 Traduction en règles et contraintes

Tous les systèmes de votes aussi bien classique avec papier ou avec enregistrement électronique ou avec connexion à une urne électronique via un réseau tel Internet, ont besoin de satisfaire à un ensemble de règles et contraintes. ***[Dictson & Ray 1]***

Après analyse et compilation, nous proposons une liste de règles et d'exigences les plus indépendantes les unes des autres, sans sacrifier à la consistance de l'ensemble.

Règle 1 : Garantir l'intimité totale de l'électeur

Définition : "l'intimité de l'électeur représente l'impossibilité de lier un vote à un électeur". L'intimité de l'électeur doit être garantie sans faille car le secret doit être assuré même si n'importe quel autre élément du système est perturbé ou endommagé, même si des personnes sont corrompues et même si les autorités ou la justice demande de fournir les données de l'élection.

L'électeur doit également être protégé après les élections pour une durée indéterminée afin de ne pouvoir mettre en doute l'intégrité de l'élection ou des prochaines qui seront organisées (exemple : influence sur un électeur pour une élection suite à la divulgation de son choix de vote lors d'une élection précédente).

Règle 2 : Garantir le secret du vote

Définition : "le secret du vote représente l'impossibilité de connaître la valeur d'un vote" Le secret du vote doit rester intact même si tous les votes et les clefs de déchiffrements sont découvertes ou identifiées suite à des actes de collusion, des attaques ou des fraudes.

Le secret ne doit pas résider exclusivement dans l'utilisation d'un protocole de communication chiffré ou encore de règles de non-collusion entre les détenteurs de clefs ou de pouvoir. Il faut combiner différents types de sécurités afin d'offrir une garantie totale de préservation du secret.

Règle 3 : Garantir l'intégrité des élections (éligibilité et unicité)

Définition : "l'intégrité d'une élection représente l'impossibilité pour n'importe quelle personne ou intervenant de modifier les résultats d'une élection, excepté par l'expression de son propre vote unique"

Tous les électeurs reconnus doivent être autorisés à voter et ne peuvent exprimer qu'un seul vote.
Le système assure que personne ne peut ajouter, modifier et supprimer un vote sans être détecté.

Règle 4 : Offrir des procédures de vérification pour l'électeur

Le système doit fournir des possibilités de vérification de l'intégrité des élections pour tous les votes acceptés et comptabilisés.

Pour chaque électeur, le procédé doit procurer une solution ou des méthodes de vérification directe afin de contrôler que son vote est bien présent ou reçu dans l'urne et qu'il sera comptabilisé une seule fois.

L'électeur ne pourra vérifier la validité de réception que de son propre vote.
De plus cette vérification informera l'électeur uniquement sur la présence de son bulletin mais pas sur le choix de vote.

Règle 5 : Offrir des outils d'audit ou de totalisation

Le système doit offrir des fonctionnalités pour l'audit et pour recompter les bulletins avec un taux d'erreurs le plus bas possible et au moins strictement inférieur ou comparable au taux habituel d'un système de vote conventionnel.

Les résultats d'audits et les preuves de votes doivent pouvoir être stockés pour ensuite être consultés et comparés pendant ou après les opérations d'élections.
Cette contrainte ne doit pas compromettre les règles d'intégrité ou d'intimité de l'électeur.

Règle 6 : Garantir l'intimité lors des contrôles et audits

Si tous les votes papiers, électroniques ou chiffrés sont contrôlés, aussi bien par une administration que par un système informatique, l'identité de l'électeur pour chaque vote ne doit pas être révélée.

Règle 7 : Garantir une élection 100% complète

Tous les votes ou absences de votes (votes blancs) doivent être correctement comptabilisés avec zéro erreur.

Règle 8 : Identifier un vote incorrect ou nul

Suivant les règles établies par le type d'élection organisé, le système doit reconnaître les choix incompatibles ou incorrects exprimés par l'électeur au moment de son vote.

Le système refusera le vote et préviendra l'électeur de son erreur sans en informer d'autres personnes.

Règle 9 : Autoriser le "Vote Blanc"

Le système doit autoriser l'électeur à choisir de voter ou de ne pas voter (vote blanc), et ceci alternativement sans limite jusqu'au moment où il confirme définitivement son choix et envoi son vote dans l'urne.

Suivant la définition des règles d'élections, le procédé peut autoriser l'électeur à exprimer un vote blanc ou encore un vote pour la totalité des choix sur le bulletin de vote.
La règle d'identification d'un vote incorrect ou nul, peut éventuellement être modifiée afin de signaler un vote nul à l'électeur mais lui permettre de confirmer son choix et donc de présenter un vote nul dans l'urne.

Règle 10 : Authentifier le modèle de bulletin de vote

Le type de bulletin de vote et son contenu peut être différent pour chaque électeur ou par type d'électeur.

A cette fin, le système doit pouvoir lier le type de bulletin à l'identifiant de l'électeur et se suffire de cette information.

Exemple : en Belgique lors de la même élection, les électeurs européens avaient accès au bulletin de vote pour les communales, mais pas au vote provincial, à la différence des citoyens belges ayants accès aux deux bulletins.

Règle 11 : Utiliser les redondances des canaux de communication

Le système doit utiliser des canaux de communication redondants et indépendants afin de garantir la validité de l'information.

L'information qui circule de manière électronique sera sécurisée, signée et chiffrée.

Si le système est connecté à un réseau, il est obligatoire de sécuriser et de solidifier les connections afin de garantir un taux d'erreur comparable ou inférieure aux échanges d'informations dans les systèmes d'élections conventionnelles.

Règle 12 : Fournir une structure de contrôle de sécurité

Le système doit offrir une structure de contrôle de sécurité pour un vote de bout en bout du circuit de l'information.

Cette structure peut, par exemple, utiliser une certification digitale au travers d'une autorité de confiance.

Le contrôle de la validité du bulletin de vote doit être indépendant des données, indépendant de la représentation et indépendant du langage utilisé.

Règle 13 : Etre indépendant de la technologie

Le système doit permettre aux votes et aux techniques de contrôles d'être utilisés par un canal classique et/ou avec connexion à un réseau type Internet.
Il doit également permettre l'utilisation de matériel informatique standard (PC) ou encore dédicacés pour installer les composants hardware ou software, seuls ou en liaison entre eux.

Règle 14 : Fournir une présentation adaptée à l'électeur

La technique doit permettre de présenter ou d'afficher le bulletin de vote en plusieurs langues, tailles ou style de caractères suivant le choix le plus confortable pour l'électeur ou suivant ses incapacités (par exemple : malvoyant), et ceci sans compromettre le procédé d'identification ou les règles globales du système d'élection.

Règle 15 : Etre ouvert sur l'extérieur (Open code)

Le système doit être définit pour permettre la connaissance, la publication et la vérification de toutes implémentations, architectures, règles de sécurité ou codes de programmes (Open code) par toutes personnes intéressées.

La disponibilité et la sécurité du système ne doivent pas être fondées sur le fait de garder les sources des programmes secrets ou d'en limiter strictement l'accès.
Ceci ne peut être garanti car les personnes qui possèdent les sources pourraient les livrer volontairement ou involontairement.

Il est également inutile de sécuriser les canaux de communications en empêchant tout attaquant d'observer la structure des messages ou les protocoles utilisés.

Le procédé requérra la propriété de "Zéro connaissance", c'est-à-dire que l'observation des messages du système n'indique aucune information sur l'architecture et les contrôles du système. Seules les clefs de chiffrement doivent être secrètes.

Règle 16 : Etre rapide pour les opérations de vote

L'électeur doit pouvoir exprimer son vote rapidement en une seule opération et avec un minimum de matériel ou de connaissance spéciale.

Règle 17 : Offrir la mobilité

Le système ne doit pas avoir de restriction, autre que la logistique, pour la localisation des bureaux de vote utilisés pour les élections.

Règle 18 : Etre efficace

Le système d'élection doit pouvoir être gérée et administrée avec un nombre raisonnable de ressources humaines et au plus égal à celles nécessaires à l'organisation d'une élection classique.

Règle 19 : Offrir la variabilité de la durée des élections

Le système pourra permettre d'étendre la durée des opérations de vote pour une élection et ceci pour une période plus ou moins longue.

La sécurité et l'intégrité du procédé seront garanties durant toute la durée de l'élection.

Règle 20 : Autoriser la modification du vote par un électeur

Le système peut permettre à l'électeur de modifier son choix de vote pendant une certaine période de temps, c'est-à-dire pendant toute la période d'ouverture des élections.

Cette règle n'est pas d'application, ni autorisée dans les élections officielles, mais uniquement envisageable pour des élections privées.
Dans les systèmes d'élections officielles, il est interdit à un électeur de revenir sur son choix une fois que celui-ci est placé dans l'urne de vote.

1.6 Types d'implémentations

La liste des exigences et des contraintes peut être utilisée pour différentes implémentations de systèmes d'élections incluant notamment les élections par réseau tel Internet. ***[Jones]***

Pour rappel, nous identifions un système de vote électronique, qui utilise des solutions informatiques sans connexion à un réseau comme "Electronic-Voting System" ou *E-Vote*, et les systèmes qui utilisent des solutions informatiques mais avec une connexion à un réseau ou à Internet comme "Internet-Voting System" ou *I-Vote*.

Chaque système d'élection possède cinq composants ou étapes :

- l'enregistrement des électeurs;
- l'identification et l 'authentification de l'électeur;
- l'isoloir ou la station pour le vote;
- l'urne;
- la totalisation des votes et la publication des résultats.

Pour chaque type d'implémentation, nous devons préciser la localisation des trois composants qui sont utilisés pendant la durée de l'élection même :

(1) L'identification de l'électeur;
(2) La station de vote;
(3) L'urne

Nous devons considérer que chacun des trois composants peut aussi bien être de type LOCAL ou à DISTANCE.

- Le type **LOCAL** identifie une présence du composant dans un bureau ou local de vote.
- Le type à **DISTANCE** identifie une connexion via un réseau pour délocaliser le composant n'importe où et, éventuellement au domicile même de l'électeur.

Les deux possibilités de localisation pour chacun des trois composants principaux permettent de classifier, l'implémentation d'un système d'élection en huit catégories comme dans le tableau suivant :

Complexité	Type d'élection	Authentification de l'électeur	Station de Vote	Urne électronique	Implémentation
Moins complexe	Dans bureau de vote	Local	Local	Local	E-Vote
	Dans bureau avec connexion au réseau	Local	Local	Distance	I-Vote
	-	Local	Distance	Local	incohérent
	-	Local	Distance	Distance	non utilisé
	-	Distance	Local	Local	non utilisé
	-	Distance	Local	Distance	non utilisé
	-	Distance	Distance	Local	incohérent
Très complexe	Ordinateur Connecté à un réseau	Distance	Distance	Distance	I-Vote

Le tableau nous indique la complexité du système pour son implémentation et sa sécurisation.

Lorsque le vote s'exécute à "Distance" alors il n'est plus cohérent que l'urne soit en "Local".

D'autres combinaisons présentées dans le tableau ne seront pas utilisées car elles ne sont pas logiques ou compliquent la procédure de vote en comparaison avec un système classique.

Plus cette complexité augmente, plus le système devra utiliser des fonctions de vérification et de redondance d'informations.

Si les redondances augmentent la fiabilité de la méthode, et si les vérifications augmentent la confiance au système, alors les risques sont réduis.

La liste des exigences et contraintes pourrait être appliquée à toutes les combinaisons avec un degré variable de risques en fonction de l'implémentation.

Nous présenterons en détails dans les chapitres 2 & 3, des exemples des différentes implémentations (E-Vote et I-Vote) utilisées ou expérimentées en Belgique, en Europe et aux Etats-Unis.

A partir de ce tableau, nous procédons à l'analyse en détail des possibilités de phases d'implémentations des systèmes votes électroniques à partir de bureaux ou de stations de vote, et également à partir de n'importe quel ordinateur connecté à un réseau, c'est-à-dire pour des élections à distance.

1.6.1 Election via des bureaux de votes

Nous pouvons envisager deux phases d'implémentation pour les organisations d'élection à partir d'un bureau de vote. ***[Turner-Drozdova]***

Les phases d'implémentations sont présentées par ordre de difficultés croissantes.

Phase 1 : Vote électronique dans un bureau de vote traditionnel

Cette implémentation utilise une configuration standard d'un bureau de vote traditionnel :

- du personnel humain qui dirige et surveille les opérations d'élection;
- une authentification de l'électeur dans le bureau;.
- un vote via une machine ou un terminal dans un lieu isolé.

Suivant que la machine à voter est reliée ou non à un réseau, l'urne (physique ou électronique) se trouvera soit dans le bureau, soit connectée à distance.

L'authentification de l'électeur peut être effectuée par les personnes responsables du bureau de vote, par exemple par un pointage dans une liste d'électeur sur papier ou en format électronique (base de données).

Le système peut également utiliser une solution pour permettre à l'électeur de s'identifier directement sur le terminal de vote qui sera relié par réseau à une base de donnée centralisée d'authentification. Cette possibilité implique le respect des règles d'authentification et d'unicité présentées précédemment.

Différentes solutions techniques existent telle que l'utilisation d'un identifiant unique, lié à un code secret personnel à l'électeur ou encore l'identification par une carte d'identité à puce électronique avec signature digitale intégrée (Smartcards).

Certains spécialistes envisagent le développement des fonctionnalités de sécurisation par Biométrie afin de permettre une reconnaissance fiable et unique de l'électeur.

Les différentes solutions présentées ici sont combinables entre elles.

L'utilisation d'un système d'identification de l'électeur se basant sur un registre centralisé et global, permet l'accès de chaque bureau à n'importe quel électeur et ceci indépendamment de son domicile ou d'autres facteurs de classifications.
Cette souplesse offerte à l'électeur dans le choix de son lieu de vote, supprime une contrainte souvent liée au déplacement pour les élections, tout en continuant à obliger l'électeur de se rendre dans un bureau de vote, mais de son choix.

Phase 2 : Vote électronique via des terminaux ou stations de vote

Cette évolution de la Phase 1 permet d'étendre les possibilités offertes par la connexion au réseau des stations de vote et la centralisation des données pour l'identification des électeurs.

L'implémentation oblige encore l'électeur à se déplacer pour effectuer son vote, mais plus dans un bureau de vote traditionnel.

En effet, cette solution propose de placer des stations ou terminaux de vote dans des lieux publics tels que les maisons communales, les bibliothèques, les établissements scolaires, les hôpitaux ou encore les locaux de grandes industries ou entreprises.

Les stations seront connectées via un réseau à un centre informatique qui recevra et totalisera les votes dans une urne électronique.
L'identification et l'accès au vote seront possibles par la connexion du terminal à une base de données centralisée des électeurs.

Le but est d'offrir la possibilité à l'électeur d'effectuer son opération de vote à proximité de son lieu de domicile, d'étude ou de travail.

Il n'y a plus de personnel humain affecté au contrôle ou à la direction des opérations de vote, car les terminaux remplissent l'ensemble des fonctions précédemment exécutées par les personnes responsables des bureaux de votes traditionnels.

Même si l'implémentation de cette solution respecte les règles d'isolement et de confidentialité, elle n'offre pas toutes les garanties contre les risques de votes sous contraintes.
Si l'isolement de la station de vote n'est pas suffisant, nous risquons de ne pas respecter la règle du secret de vote. Par exemple, une caméra de surveillance dans un lieu publique qui enregistre les opérations sur la station de vote ou encore une personne qui regarde par-dessus l'épaule de l'électeur pour consulter le choix affiché sur l'écran de la station.

Pour les deux phases d'évolution du vote à partir de bureaux, il est important de préciser que l'implémentation du système est contrôlée de bout en bout par l'architecture développée pour l'élection.

Même avec l'utilisation de stations de vote électronique et la connexion à un réseau, le procédé autorisera uniquement des connections et des échanges d'informations entre les composants connus et faisant partie de l'architecture définie (station de vote et urne électronique).

Tous les composants matériels et logiciels auront étés vérifiés, standardisés et sécurisés.
Tous sont sous le contrôle et la gestion de l'organisation des élections.

1.6.2 Election à distance

Les organisations d'élections à distance, autorisent l'électeur à voter à partir de n'importe quel ordinateur personnel relié à un réseau de type Internet, et ceci n'importe où dans le monde.

Certains experts analysent cette situation comme une alternative au vote par courrier qu'autorise certaines législations d'élections, notamment aux Etats-Unis.

Dans ce type d'élection à distance, seul un site informatique centralisé et ses éventuelles copies de sauvegarde (back up system), devra être certifié, installé et être sous le contrôle unique des organisateurs des élections.

Le rôle de ces centres informatiques sera l'authentification de l'électeur, l'envoi du bulletin de vote vers l'électeur et la réception du vote en vue de le totaliser. En fin d'élection, le centre fournira les résultats.

Les serveurs du centre informatique des élections devront autoriser les connections des ordinateurs personnels des électeurs au travers d'un réseau public comme Internet. Ils devront authentifier les électeurs et éventuellement les autoriser à poursuivre les opérations de vote.

L'envoi d'informations au travers d'un réseau vers un ordinateur inconnu, aussi bien au niveau de son architecture matérielle ou logicielle, ouvre la porte aux risques d'attaques et aux problèmes de sécurités.
En effet, ce type d'implémentation ne donne pas, aux autorités qui organisent les élections, le contrôle total de l'infrastructure utilisée de bout à bout du procédé d'élection.

Pour l'instant, aucune législation d'élections officielles, aussi bien européenne qu'ailleurs dans le monde, n'autorise ce type d'implémentation d'élection à distance.
Par contre, des expériences pour des élections privées sont déjà mises en place et utilisent le réseau Internet comme moyen de communication.
Il est donc intéressant de présenter les phases d'implémentation envisagées par certaines études publiées sur le sujet.

Nous pouvons également envisager deux étapes d'implémentation pour les systèmes d'élection à distance.

Les phases d'implémentation sont présentées dans l'ordre de difficultés croissantes.

Phase 1 : Election à distance pour un groupe d'électeurs sélectionnés.

Le principal avantage du vote à distance est de ne plus avoir de contraintes géographiques pour que l'électeur accède au vote.

Cette première phase d'implémentation du vote à distance a pour but de s'adresser aux électeurs, qui de par l'éloignement de leur pays, ne peuvent habituellement participer aux élections, si ce n'est que par l'utilisation de règles spéciales telle que la procuration ou le vote par courrier, si la législation l'autorise.

Les groupes ciblés sont par exemple, les expatriés qui gardent leur nationalité ou les employés de multinationale en poste à l'étranger.

Phase 2 : Election à distance offerte à tous les électeurs.

Cette seconde phase d'implémentation du vote à distance doit permettre à tous électeurs de voter à partir de n'importe quel ordinateur personnel connecté à un réseau public comme Internet.

L'électeur doit être identifié par un code secret et une signature digitale unique qui lui sera fournie par l'organisateur des élections.

Pour avoir confiance en l'intégrité du vote, l'électeur souhaitera utiliser un système d'élection à distance qui aura été certifié et sécurisé afin de pouvoir voter au travers d'une connexion à un réseau.

Assurer l'intégrité d'une élection devient complexe quand le bulletin de vote est envoyé via un réseau sur des ordinateurs personnels qui ne sont pas dans un bureau de votes ou sous le contrôle des organisateurs des élections.

Nous ne pouvons être certains que le bulletin de vote sera présenté correctement sur l'écran de l'ordinateur de l'électeur, aussi bien à cause d'attaques qui risquent de modifier l'information envoyée que de problèmes propres à l'ordinateur utilisé.

Il est impossible de connaître l'ensemble des ordinateurs, périphériques, logiciels, systèmes d'exploitations, cartes graphiques, écrans….. utilisés par les électeurs.

Il sera donc encore plus complexe de créer un système respectant l'ensemble des règles de sécurité et d'intimité.

Ces types d'implémentations de vote à distance n'offrent aucune garantie pour le respect des règles du secret de vote, collusion ou intimidation de l'électeur.
Pour rappel, ces règles sont le fondement même pour l'organisation d'élections officielles.

1.7 Principes de sécurisation des données.

Il est intéressant de rappeler et de définir les techniques de protection des données à l'aide de la signature digitale et de la certification. ***[Adler 2000a]***

L'idée est de fournir une présentation non exhaustive mais qui permet de bien assimiler les principes de bases des techniques applicables dans les systèmes d'élections électroniques.

1.7.1 Sécurisation à l'aide d'une clef

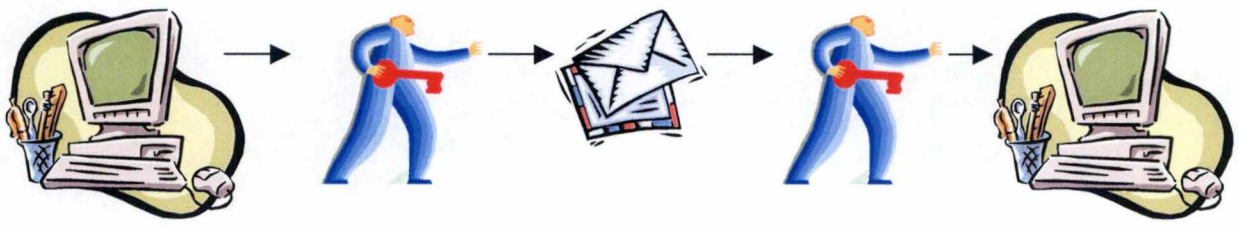
Lorsque nous souhaitons protéger quelque chose que ce soit une voiture, de l'argent ou encore une personne, nous le placerons dans un endroit fermé à clef.
C'est donc la personne qui possède la clef qui peut récupérer le bien ainsi protégé.

Un système de sécurisation des données utilisant une clef de chiffrement symétrique est construit sur le même principe, de telle sorte, que personne ne peut accéder ou lire les données chiffrées sans posséder la clef de déchiffrement.

Le fait de posséder ou de connaître la clef est donc la solution pour briser le secret de chiffrement des données.

Cette architecture utilise la même clef pour procéder au chiffrement et au déchiffrement de l'information à protéger.

Illustration du protocole de chiffrement symétrique à une clef.



Ordinateur de Alice — ***Chiffrement avec la clef secrète*** — ***Message sécurisé*** — ***Déchiffrement avec la clef secrète*** — ***Ordinateur de Bob***

1.7.2 Protocole de chiffrement symétrique

Le chiffrement symétrique utilise une clef numérique très longue qu'il est presque impossible de deviner.

Cette idée est comparable à l'utilisation d'une clef de voiture ou de maison dont le dessin ou la forme est complexe et difficile à reproduire.

La longueur habituelle d'une clef digitale varie de 56 à 128 bits.
Une clef à 56 bits peut représenter 2^{56} ou 72 millions de milliard de combinaisons différentes.
Pour une clef de 128 bits, nous portons ce chiffre à 2^{128} ou 340 millions de milliard de combinaisons différentes.

Le protocole est identifié comme symétrique lorsque le chiffrement et le déchiffrement des données se basent sur la même clef.

Les clefs symétriques présentent le même problème ou risque que pour les portes classiques, à savoir que n'importe quelle personne qui obtient la clef peut ouvrir et visualiser le document chiffré.

La protection repose donc sur le secret de la clef qu'il faut garder intact, mais ceci est un vrai challenge lorsque nous connaissons les faiblesses humaines.

L'avantage de cette architecture est que l'algorithme de chiffrement symétrique est efficace et très rapide. Cette technique simple autorise des capacités de chiffrement exprimées en dizaines de méga bytes par seconde.

Il existe sur le marché plusieurs algorithmes symétriques de qualités tels que DES, Blowfichn IDEA et RC5.

1.7.3 Sécurisation à deux clefs

Pour contrer les problèmes posés par la protection symétrique, c'est-à-dire une seule et même clef, nous pouvons envisager un système utilisant deux clefs.

L'idée est d'utiliser une clef pour verrouiller ou chiffrer l'information et une seconde clef pour la déverrouiller ou déchiffrer.

Cette solution signifie que la clef de verrouillage peut être en possession de n'importe qui, mais que seul le destinataire du message doit posséder la clef de déverrouillage.

Pour chiffrer une information ou un message que quelqu'un souhaiterait communiquer, l'émetteur devra utiliser la clef "de chiffrement" du récepteur et ensuite lui envoyer le message ainsi chiffré.

Si une autre personne que le récepteur prévu, intercepte le message lors du transfert, il lui sera impossible de le déchiffrer sans être en possession de la clef de "déchiffrement " personnelle du récepteur.

En fait, une fois que l'émetteur a "verrouillé" un message, il ne pourra plus le "déverrouiller" et seul le récepteur en possession de la clef de déchiffrement en aura les moyens.

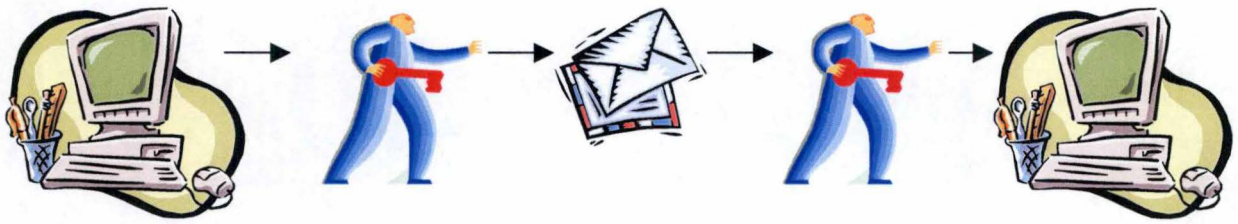
- La clef de verrouillage, chiffrement est appelée ***CLEF PUBLIQUE***
- La clef de déverrouillage, déchiffrement est appelée ***CLEF PRIVEE***

Les clefs publiques et privées sont mathématiquement liées de telle sorte qu'une clef privée peut uniquement déchiffrer les messages qui ont été chiffrés par la clef publique qui lui est associée.

De plus, il est extrêmement difficile de retrouver la valeur d'une clef privée à partir de la valeur de sa clef publique.

Le grand avantage de cette architecture appelée également PKI, c'est qu'il n'est pas nécessaire de partager un secret entre différentes personnes.

Illustration du protocole de chiffrement à deux clefs.



Ordinateur de Alice — ***Chiffrement avec la clef publique de Bob*** — ***Message sécurisé*** — ***Déchiffrement avec la clef privée de Bob*** — ***Ordinateur de Bob***

Ce protocole impose l'utilisation de clefs dont l'algorithme repose sur des clefs de très grandes tailles, c'est-à-dire entre 500 et 2000 bits.

Dans la pratique, l'utilisation d'un protocole de chiffrement à deux clefs est beaucoup moins rapide qu'un protocole symétrique à clef unique.

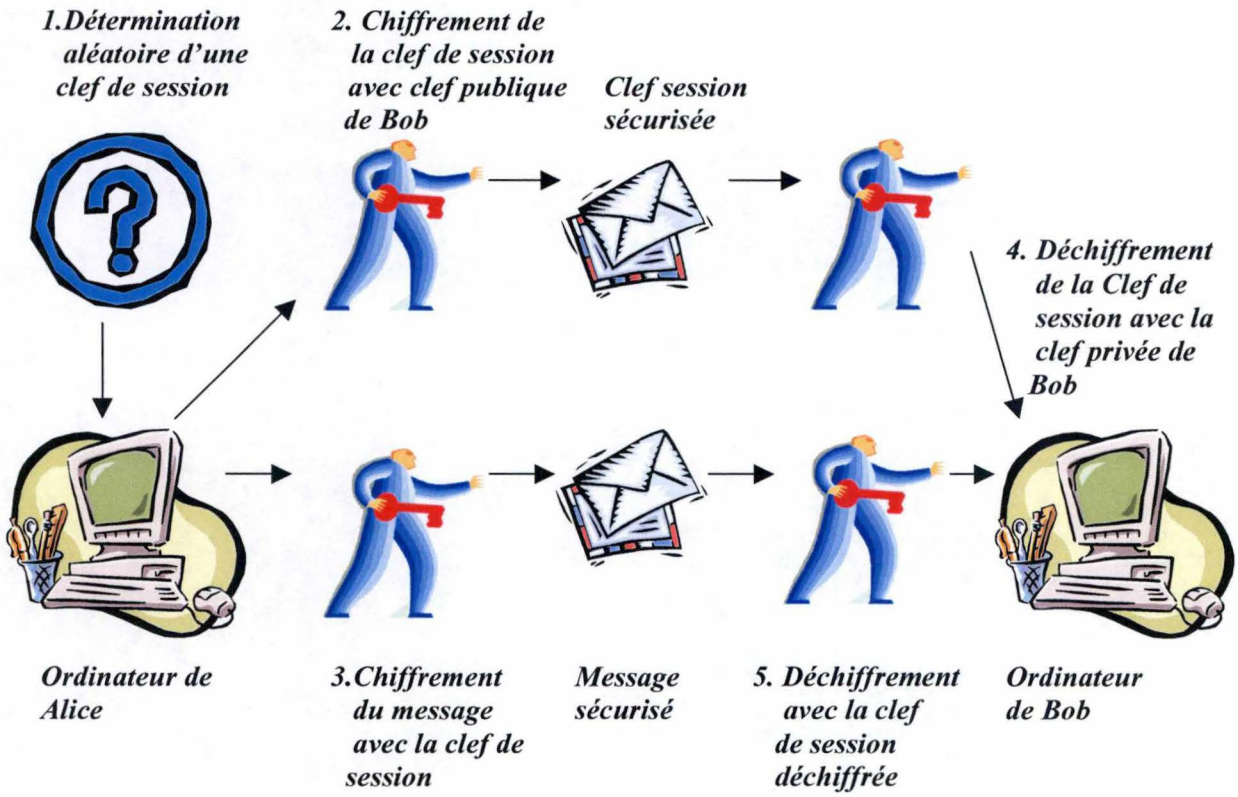
Une solution mixte peut être développée de telle sorte que lorsque l'on chiffre un document de grande taille, il est préférable d'utiliser l'algorithme de chiffrement à clef symétrique qui est plus rapide.

1. L'algorithme symétrique utilisera une clef générée aléatoirement et appelée "Clef de Session" pour chiffrer le message.
2. Ensuite cette "Clef de Session" est elle-même chiffrée en utilisant la "Clef Publique" du receveur du message, c'est-à-dire à l'aide de l'algorithme à deux clefs.
3. Etant donnée la petite taille de la clef symétrique dite "de Session", typiquement moins de 30 bytes, son chiffrement avec le protocole à deux clefs sera très rapide malgré la relative lenteur de l'algorithme.
4. Le document chiffré et la "clef de session" chiffrée sont envoyés au destinataire prévu du message.

5. Le receveur déchiffre la "clef de session" à l'aide de sa clef privée et utilise ensuite la "clef de session" lisible pour déchiffrer le document à l'aide du protocole de clef symétrique.

Cette solution ou architecture mixte, a pour but de parer au problème de la durée de chiffrement de longs messages dans une architecture à deux clefs (publique et privée), tout en utilisant une solution qui ne partage pas un secret.

Illustration du protocole de chiffrement mixte



1.7.4 Qu'est-ce que la certification ?

Pour présenter la certification, nous procédons à l'analyse du problème suivant :

> Une personne souhaite envoyer un document chiffré avec le protocole à deux clefs et donc utiliser la clef publique du destinataire.
>
> Pour rappel, c'est l'émetteur qui utilise la clef publique du récepteur pour chiffrer le document à envoyer et c'est le récepteur, à l'aide de sa clef privée qui déchiffre le document reçu.
>
> Comment un émetteur peut-il connaître et recevoir la clef publique du récepteur ?
>
> Malgré que cette clef soit de très grande taille, nous pouvons imaginer que celle-ci serait communiquée par téléphone ou courrier a l'émetteur par le récepteur propriétaire.
>
> Cette solution fonctionne et ne pose pas de problème de sécurité, car il n'y a pas de secret dans le fait de découvrir une clef publique.
>
> Dans le cas ou la clef publique reçue est erronée ou modifiée de manière intentionnelle, nous aurons alors un message chiffré qu'il sera impossible de déchiffrer avec la clef privée du récepteur.
>
> N'oublions pas que clef publique et clef privée sont indissociables pour effectuer correctement les processus de chiffrement et de déchiffrement .
>
> Le risque est encore plus grand si un émetteur utilise de bonne fois la clef publique qu'il pense être associé à un récepteur, mais qui est en réalité celle d'un "pirate" ou d'un conspirateur qui de ce fait arrive à la tromper.
> Si le message ainsi chiffré est intercepté par ce même "pirate", il pourra alors le déchiffrer sans problème avec sa clef privée.
> Même si le récepteur initialement prévu reçoit le message ou une copie, il ne pourra le déchiffrer avec sa clef privée, car ce n'est pas sa clef publique qui a été utilisée lors du chiffrement.

Le problème de sécurité repose sur le fait qu'il n'y a pas d'association entre une personne et sa clef publique.

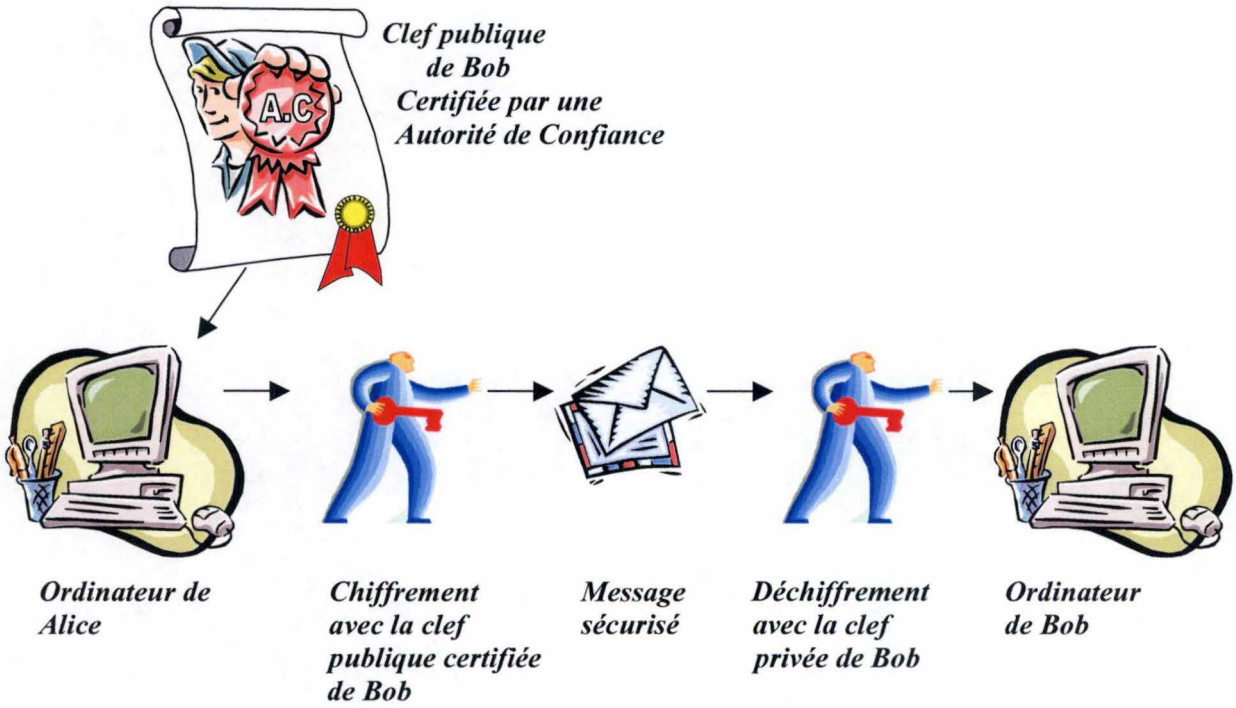
C'est pour cette raison que le principe de ***certificat*** a été développé.

Pour "certifier" la validité d'une clef publique, il est nécessaire au départ, de demander à une entité neutre et de confiance, de vérifier l'identité d'un récepteur et d'y associer sa clef publique.

Cette entité de confiance est reconnue comme une "Autorité de Certification" (A.C.) ou encore un "Notaire".

Une fois qu'une personne a prouvé son identité à l'Autorité de Certification, celle-ci reliera sa clef publique à son identité et ***"signera" de manière digitale*** le résultat pour fournir un **Certificat digital signé.**

Illustration du protocole de chiffrement à deux clefs avec certificat.



Le certificat offrira la confiance en la validité d'une clef publique, à tous les émetteurs souhaitant l'utiliser. Cette certification relie de manière sécurisée une clef publique à son propriétaire identifié.

1.7.5 La signature digitale

Qu'est ce que la signature digitale d'un message ?

A l'aide de la certification, nous avons trouvé une solution pour garantir qu'un message chiffré ne pourra être lu que par le destinataire choisi par l'émetteur.

Mais comment pouvons-nous garantir que le contenu du message n'aura pas été modifié pendant la transmission ?

Avec le protocole de chiffrement utilisant les clefs publique et privée, nous pouvons appliquer la technique de "Hashing".

La technique de "Hashing" calcule une "empreinte digitale" ou "hash value" à partir d'une "série de bits".

Cette "série de bits" peut être prise au hasard dans un document ou message électronique.

Le calcul de l'empreinte digitale d'un message possède les propriétés suivantes :

- la probabilité que le calcul de l'empreinte digitale de deux "séries de bits" soit identique est très proche de zéro;

- il est impossible de reconstruire ou de déterminer la valeur de la "série de bits" à partir de l'empreinte digitale calculée. C'est donc un processus irréversible.

Si nous possédons "l'empreinte digitale" d'un document, nous sommes alors capables de détecter toutes modifications car l'empreinte sera également modifiée.

- L'auteur d'un document ou d'un message peut calculer et générer ***l'empreinte digitale***.
- Cette empreinte sera chiffrée à l'aide du protocole à deux clefs et en utilisant la ***clef privée de l'auteur*** du message.
- Le résultat du chiffrement de l'empreinte produira la ***signature digitale***.
- Cette signature digitale accompagne alors le document ou le message lors de sa transmission, de ce fait nous pouvons expliquer la notion de ***message signé***.
- Le récepteur peut déchiffrer la signature à l'aide de la clef publique de l'émetteur et ainsi révéler l'empreinte digitale du document à l'origine de la transmission.
- Il est encore nécessaire de recalculer l'empreinte du document reçu et de la comparer avec la valeur de l'empreinte envoyée dans la signature chiffrée.
  En cas de différence, la validité du message sera mise en doute et la corruption aura été détectée.

Les certificats envoyés par les autorités de certifications seront signés de manière digitale afin de garantir et vérifier la validité du contenu.

Une autre fonctionnalité de la signature digitale est la non-répudiation des messages signés. En termes clairs, il sera impossible à un signataire de déclarer par la suite qu'il ne l'a pas fait.

En fait, la signature digitale est un acte privé qui est exclusivement réservé au propriétaire d'une clef privée, dénommé le signataire.

1.7.6 Protection de la clef privée

Etant donnée qu'une clef privée permet de déchiffrer et signer un document, sa protection et son secret ont une très grande importance.

Typiquement, la clef privée d'une personne est stockée sur le disque dur de son ordinateur personnel et son accès est protégé par un code secret.

Cette place typique pour le stockage de la clef privée est dangereuse car cette clef pourrait être trouvée et divulguée par des attaques de styles virus ou espionnage au travers du réseau lors de la connexion de l'ordinateur.

La meilleure solution est donc de placer la clef privée sur un support détachable et indépendant comme par exemple une disquette ou une carte à puce électronique (Smartcards).

De plus, l'accès au fichier ou au support contenant la clef privée sera également sécurisé par une identification unique et personnelle, comme un code secret (PIN Code).

L'utilisation d'un média indépendant à accès sécurisé pour stocker la clef privée offre donc une double protection car l'utilisation de la clef demande de posséder le média de stockage et le code secret d'accès.

Nous pouvons imaginer une solution garantissant encore plus de sécurité que l'utilisation d'un code secret qui pourrait être éventuellement identifié.

En effet, les techniques nouvelles de ***signatures Bio métriques*** permettent de donner accès au média sur base de l'identification unique d'éléments humains personnels au propriétaire, telles que les empreintes digitales, le dessin de l'iris de l'œil, le réseau veineux de la rétine, les caractéristiques de la voix, la forme de la main, les traits du visage ou éventuellement des informations génétiques.

L'application au vote électronique de cette technologie, demande la modification de certaines législations éthiques car elle implique la détention d'une base de données globale avec l'ensemble de données privées et bio métriques de tous les citoyens (par exemple : empreintes digitales).

Certaines sociétés commencent à commercialiser des périphériques pour l'identification bio métrique et certains logiciels ou systèmes d'exploitations utilisent de telles reconnaissances pour autoriser les accès.

Le 20 juillet 2001, la Belgique vient d'adopter une loi autorisant le développement et la distribution d'une carte d'identité nationale contenant une puce électronique (Smartcards).
Cette puce contiendra différentes informations et notamment la signature électronique (clef privée) personnelle du citoyen. L'accès à la clef privée sera sécurisé par un code secret individuel.
La signature électronique sera exigée dans un premier temps pour la commande et l'envoi de certains documents officiels par Internet, telle que la déclaration d'impôt.
Un budget de dix millions d'Euros a été alloué pour la mise en place d'une phase de test reprenant les 330.000 Belges de onze communes (une par province et une commune bruxelloise).
Les cartes seront distribuées à partir du premier trimestre 2002.
Le ministère des Affaires intérieures souhaite généraliser la carte d'identité digitale pour 2005.

1.7.7 Synthèse de la sécurisation des données.

Nous pouvons synthétiser l'emploi des clefs et protocole de chiffrement pour la sécurisation des données par le respect des règles suivantes :

- Chiffrement des messages et documents pour empêcher la lecture ou consultation par une autre personne que le destinataire.
- Signature digitale des messages et documents pour valider leur contenu après la signature.
- Protection et secret de la clef privée.
- Disponibilité d'une autorité de certification pour attester de la validité des identités digitales et des clefs publiques.
- Utilisation d'une clef privée pour déchiffrer un message ou pour le signer.
- Utilisation de la clef publique pour chiffrer un message ou vérifier une signature.

1.8 Sécurité du vote dans les systèmes d'élections I-Vote

Il existe énormément d'études et d'articles sur le sujet de la sécurité des systèmes de votes électroniques connectés à un réseau ou simplement les systèmes de *I-Vote*.

Il existe donc de nombreuses solutions pour l'implémentation et l'architecture de tels systèmes.

Depuis plus de vingt ans, des recherches sur les protocoles de chiffrement sont entreprises afin de répondre aux exigences des systèmes d'élections pour le respect des règles de secret et d'intégrité. ***[Adler 2000b]***

Le problème fondamental des différentes études est le conflit entre la résolution simultanée des exigences pour le respect du secret d'un vote et celles sur l'intégrité des élections.

Si un système se penche pour une solution très sécurisée pour une des deux exigences, ce même système échoue ou présente des faiblesses pour l'autre.

Par exemple, si le vote est maintenu secret en éliminant l'information sur l'identité de l'électeur, alors l'intégrité de l'élection est compromise car il y a un risque de possibilité d'ajout, de modification ou de suppression de bulletins de votes anonymes.

D'autre part, si la solution privilégie une technique efficace pour l'audit et le contrôle des votes exprimés, alors nous sommes souvent confrontés à un risque de violation du secret de vote.

Il est donc intéressant de synthétiser les problèmes identifiés et les solutions proposées pour sécuriser et assurer l'intégrité des votes dans les systèmes d'élections électroniques lorsque ceux-ci sont connectés à un réseau.

Observons plus concrètement les éléments suivants :

- la sécurisation du vote envoyé sur le réseau;
- la sécurisation du vote au centre informatique des élections;
- la sécurisation du vote sur le terminal ou ordinateur de vote;
- la sécurisation du vote par chiffrement homomorphique.

TERMINAL DE VOTE

CENTRE INFORMATIQUE DES ELECTIONS

1.8.1 Sécurisation du vote envoyé sur le réseau

Quand un bulletin de vote voyage de manière électronique au travers d'un réseau informatique, il est important de garantir que personne ne pourra intercepter l'information pour la consulter, la modifier ou encore la supprimer.

Une des attaques des connexions via le réseau Internet qui a pour but de détourner l'émetteur vers un autre site récepteur, se nomme "Web Spoofing". ***[Felten & Balfanz]***
Le "Web Spoofing" trompe le client en le connectant à un faux partenaire qui copie en apparence le site auquel souhaite accéder le client.
Ce type d'attaque permet de surveiller les clients connectés, mais également de modifier leurs messages ou requêtes originales et ensuite de les transmettre au destinataire initialement prévu.
Imaginons cette attaque dans le cadre des élections électroniques et nous comprendrons aisément les risques liés à ce type de tromperie.

Il existe aussi des variantes aux attaques Web Spoofing, telles que TCP et DNS Spoofing.
Dans le TCP Spoofing, les paquets d'informations sont envoyés sur le réseau avec des adresses de retour modifiées.
Dans le DNS Spoofing, l'attaquant modifie l'information sur l'adresse IP du réseau Internet qui correspond au nom logique d'une machine ou d'un serveur.

La connexion via un VPN (Virtual Private Network) et l'utilisation du protocole SSL (Sécure Sockets Layer) qui protège les transactions d'E-Commerce sur Internet, peuvent être utilisés pour protéger le vote électronique contre l'interception ou la modification lors de son transfert entre le terminal de vote et les serveurs du centre informatique des élections. ***[Guill.net]***

Pour rappel, le protocole SSL utilise les fonctionnalités offertes par TCP/IP (Network layer) pour permettre aux couches supérieures (par exemple : HTTP Application layer) d'accéder à un mode d'accès sécurisé.
Les trois fonctionnalités de SSL sont, l'authentification du serveur, l'authentification du client et le chiffrement des données. ***[Guill.net]***
Un VPN est une liaison sécurisée entre deux parties via un réseau public, en général Internet.
Le principe du VPN est basé sur la technique du "tunnelling". Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Ensuite la source chiffre les données et les achemine en empruntant ce chemin virtuel.
Cette technique assure l'authentification des deux parties, l'intégrité des données et le chiffrage de celles-ci.

Les techniques de sécurisation du réseau avec SSL et VPN, garantit que l'électeur est connecté correctement aux serveurs du centre informatique, que l'intégrité des données est assurée et qu'il ne sera pas détourné vers un autre centre ou site "pirate".

Même si l'infrastructure sécurise la connexion, entre l'émetteur d'un vote électronique et les serveurs au centre informatique des élections, à l'aide des techniques VPN et SSL, cette solution est malgré tout incomplète.

En effet, le secret de vote est encore en danger par des attaques effectuées sur le terminal ou ordinateur de vote, et sur les serveurs du centre informatique des élections.

1.8.2 Sécurisation du vote au centre informatique des élections

Tous les systèmes de votes doivent empêcher les fraudes d'initiés ou de corruption et de collusion.

Ces types de fraudes représentent la plus grande menace pour l'intégrité des élections.
S'il est possible de subordonner un employé ou un responsable des élections et que celui-ci a la possibilité de changer les résultats, alors nous détruisons totalement la confiance dans l'intégrité des élections.
De plus, rien ne sert de sécuriser le système contre les attaques extérieures si le plus grand danger de fraude se situe à l'intérieur.

Pour combattre les fraudes internes et externes, les systèmes d'élections traditionnelles "papier" distribuent la confiance et les possibilités d'actions à différentes personnes de catégories ou milieux différents (fonctionnaires, observateurs des partis, personnes civiles...)

Il est donc impossible de compromettre une élection en agissant sur une seule personne.
La division des responsabilités et la multiplicité des catégories garantissent que toutes tentatives de fraude seront détectées et déclarées.

Les systèmes de votes électroniques imitent cette technique et l'applique aux responsabilités et sécurités informatiques, notamment contre la corruption des informaticiens responsables des développements des logiciels et de la mise en place de l'infrastructure.

Lorsque des protocoles de chiffrement sont utilisés, la clef de déchiffrement est divisée et distribuée à différents acteurs ou responsables des élections.
De plus, toutes les opérations de déchiffrement demandent l'introduction simultanée de toutes les parties de la clef de déchiffrement et donc, l'intervention et l'accord de plusieurs personnes.

Certaines techniques de chiffrement permettent de comptabiliser les votes sans devoir déchiffrer l'information et fournissent un résultat global chiffré.
Ce résultat global sera consultable uniquement par l'introduction simultanée de plusieurs parties de la clef de déchiffrement (voir protocole Homomorphique).

De plus, les systèmes de votes électroniques protégeront le matériel et les logiciels des attaques par des techniques et procédures de sécurisation (p.e. logiciel antivirus, Firewall, Proxy,...).

Il y aura eu certification et vérification du matériel et des logiciels avant le début des élections par une autorité de contrôle indépendante et de confiance.

Le bulletin vote électronique sera sécurisé par une authentification forte de l'électeur, le chiffrement et la signature digitale.

Un vote ne pourra être ajouté dans l'urne électronique qu'à moins qu'il soit signé de manière digitale par un électeur identifié et reconnu valide.

Cette signature digitale du bulletin empêchera également la modification d'un vote et son reniement par l'électeur.

La suppression des votes dans l'urne après sa réception pourra être impossible par l'écriture des bulletins acceptés directement sur un support mémoire ou média indélébile et stable (p.e. CD-ROM).

1.8.3 Sécurisation du vote sur le terminal ou ordinateur de vote

Il nous faut différencier les problèmes de secret et d'intégrité qui peuvent se présenter sur des machines ou terminaux de votes, suivant que :

- N'importe quel ordinateur, sans en connaître la configuration logicielle ou matériel, peut être utilisé pour se connecter au réseau et effectuer les opérations de vote.
- Le matériel et les logiciels ont été installés et configurés par les organisateurs des élections. Ils sont donc sous le contrôle total de l'infrastructure déployée.

.1.8.3.1 Sécurisation du vote sur un ordinateur quelconque

Dans le cas où la solution de vote électronique mise en place et offre la possibilité à n'importe quel ordinateur personnel de se connecter au système via un réseau, nous sommes confrontés à des difficultés de sécurisation du vote, dues à la multiplicité des systèmes et des configurations existantes sur le marché de l'informatique personnelle.

Nous ne pouvons connaître à l'avance le type ou l'état du matériel au moment de la connexion au système de vote.

Qu'en est-il du type ou de la version du système d'exploitation utilisé, quel sera le type de navigateur, est-ce qu'un logiciel de protection contre les virus est actif et à jour....
Ce sont des questions dont le domaine de réponse est trop vaste à appréhender.

Confronté à tellement d'interrogations, les risques d'instabilité et d'attaques dans une telle infrastructure sont très importants.

Actuellement, les solutions employées pour le commerce électronique par Internet (E-Commerce) sont confrontées aux même problèmes.

Différents protocoles et techniques ont été développés pour par exemple, "télécharger" en local sur l'ordinateur du client la totalité des logiciels ou modules de contrôles nécessaires aux opérations de sécurisation et d'exécution du commerce électronique.
Le module qui est téléchargé, englobe les règles de contrôle et de sécurisation pour les transactions commerciales électroniques.

Cette technique de téléchargement en local sur l'ordinateur du client, de l'ensemble des éléments logiciels nécessaire à la bonne exécution des opérations commerciales, est dénommée ***"l'approche Wallet"*** dans le cadre du E-Commerce.

Cette technique Wallet pourrait être adoptée par les systèmes de votes électroniques autorisant les opérations de vote à partir de n'importe quel ordinateur personnel connecté au réseau.

L'objet téléchargé sur l'ordinateur de l'électeur englobe alors une structure de contrôle de la communication entre le serveur du centre informatique des élections et l'ordinateur de vote.

L'ordinateur de vote chez l'électeur a besoin uniquement d'accéder aux méthodes liées à l'objet téléchargé afin d'effectuer les opérations nécessaires au vote et au chiffrement des données.

Mais cette technique "Wallet" a déjà démontré ses limites et ses problèmes lors de l'exploitation par les systèmes de commerce électronique.

Notamment la durée et la taille de l'objet à télécharger sur l'ordinateur de l'utilisateur, qui peut dépasser plusieurs centaines de kilo bytes.
Il existe aussi des problèmes liés à la version du navigateur utilisé ou aux conflits provoqués par la présence de certains logiciels ou de pilotes de périphériques.

De plus pour que l'objet téléchargé fonctionne correctement, il ne faut pas d'interruption de la connexion pendant le téléchargement.

Malgré le grand nombre de problèmes connus et pouvant compromettre la validité d'une opération de E-Commerce, cette solution est utilisée par les sociétés de commerce électronique.
En effet, les sociétés de commerce acceptent ce risque dans le cadre du *"coût et risque lié au business"*.
Il suffit alors au commerçant électronique de se protéger à l'aide d'un contrat d'assurance couvrant les paiements électroniques perdus ou encore le mécontentement des clients non livrés.

Une telle protection des failles du système par un contrat d'assurance n'est pas envisageable dans le cadre d'une solution pour le vote électronique lors d'une élection officielle.

Pour le moment, il n'existe aucune solution à valeur de risque zéro pour les implémentations autorisant la connexion de n'importe quel ordinateur au système de vote à distance.

.1.8.3.2 Sécurisation des ordinateurs et terminaux propriété du système d'élection

Comme pour tout ordinateur personnel, les terminaux et ordinateurs de vote connectés à un réseau sont sujet à différentes attaques.

Les buts de ces attaques sont :

- soit de modifier ou d'identifier les votes des électeurs exprimés localement.
- soit de mettre hors service la machine ou les logiciels de vote par des attaques de type "Denial Of Services" (DoS). ***[Guill.net]***

Nous pouvons rencontrer la panoplie complète des types d'attaques depuis la corruption du code à l'implémentation d'un code malveillant par un programmeur corrompu (attaque MalWare ou VandalWare).

L'électeur, tout en ayant confiance au procédé et au logiciel utilisés, peut être confronté à l'utilisation d'une infrastructure corrompue dans l'ignorance la plus totale.

Etant donné que l'organisation des élections identifie, configure et installe l'ensemble des terminaux ou ordinateurs de vote, il est plus facile de mettre en place des procédures et outils de sécurisation de l'architecture.

Nous pouvons énumérer quelques exemples de techniques et méthodes de sécurisation à appliquer par les organisateurs des élections. ***[Adler 2000b]***

- ***Installation à vide.***

  Après formatage de tous les supports de mémoires auxiliaires, initialiser les ordinateurs et terminaux à voter à partir d'un média inviolable (p.e. CD-ROM), pour charger et installer le système d'exploitation et les logiciels des opérations de vote.
  Cette procédure d'installation des logiciels sur du matériel vierge et standardisé sera également accompagnée d'une analyse et d'un nettoyage éventuel du BIOS.

  BIOS *(**B**asic **I**nput **O**utput **S**ystem) est un des composants vitaux de l'ordinateur. En fait, il s'agit d'un logiciel intégré dans une mémoire morte de la machine et qui a les fonctionnalités de vérification du bon fonctionnement de certains éléments physiques au démarrage de la machine et ensuite le lancement du système d'exploitation.*

- ***Essais statistiques.***

  Avant ou pendant les opérations d'élections, choisir au hasard des ordinateurs de votes en fonctionnement pour vérifier et mesurer l'exactitude des processus de vote.

- ***Matériel spécial sécurisé.***

  Développer et fabriquer des terminaux, avec des caractéristiques techniques inhabituelles, adaptées à la sécurisation du vote électronique et non présentes dans un ordinateur personnel grand public

  Par exemple :

  - code du programme résidant dans une mémoire stable et inviolable;
  - ne pas équiper le terminal de support mémoire physique (disque dur);
  - spécificité technique du matériel (absence de clavier ou de bouton on/off).

Enfin, lors de l'envoi d'un bulletin de vote électronique entre la station de vote de l'électeur et l'urne électronique dans le serveur du centre informatique des élections, il faut garantir la bonne réception du vote dans l'urne.

Des règles de sécurités dans l'échange d'information doivent être établies en retournant à l'électeur un "signe" de confirmation de bonne réception du bulletin par le serveur, et ceci sans compromettre le secret du vote.

Les techniques de chiffrement, de signature et de certification de message seront toujours d'application.

1.8.4 Sécurisation du vote par chiffrement homomorphique

Les techniques de chiffrement ont pour but de garantir le secret d'un vote.

Lorsque le bulletin de vote chiffré est reçu par l'urne électronique dans le centre informatique des élections, il faut le déchiffrer pour interpréter le choix de l'électeur et opérer les opérations de totalisation.

Afin de pouvoir garantir des contrôles et audits pour assurer la validité des élections, il est intéressant que l'identifiant de l'électeur accompagne son vote de manière chiffrée. Mais cette solution n'offre pas assez de garanties pour l'intégrité des élections car il existe une possibilité de visibilité de l'identité de l'électeur lors des opérations de dépouillements.

Il existe une parade à cette problématique par l'utilisation de la technique du protocole de chiffrement homomorphique. ***[VoteHere]***

Si la signature digitale assure la validité des élections, le chiffrement homomorphique permet de garantir le secret du vote des électeurs.

Le chiffrement homomorphique est une technique spéciale de chiffrement qui a la propriété que la somme de deux nombres chiffrés est toujours égale au chiffrement de leurs sommes.

Cela signifie que n'importe qui peut calculer et vérifier la "somme chiffrée" d'un ensemble de valeurs chiffrées.
Comme les données sont chiffrées, on ne peut pas connaître réellement quelles sont les valeurs chiffrées, aussi bien pour l'ensemble des valeurs initiales que pour la somme finale.
Si la valeur finale est déchiffrée alors le résultat est également correct.

Dans le cadre des votes électroniques, le chiffrement homomorphique autorise le dépouillement et la comptabilisation des bulletins de votes sans devoir déchiffrer le message électronique envoyé par l'électeur.

Les résultats finaux de la totalisation sont également retournés chiffrés par le système informatique aux organisateurs de l'élection.

Seule l'utilisation simultanée de toutes les clefs de déchiffrement, en possession de plusieurs responsables, pourra déchiffrer et afficher le résultat des élections "en clair".

La technique de chiffrement homomorphique ne fonctionne que pour des choix de vote identifié pour oui/non ou 1/0 ou vrai/faux, c'est-à-dire binaire.
Il n'est donc pas possible d'utiliser cette technique lorsque l'électeur peut indiquer un choix plus complexe ou multiple comme par exemple lors des référendums.

.1.8.4.1 Scénario d'une élection électronique utilisant le chiffrement homomorphique

Sans être exhaustif, nous pouvons identifier les grandes étapes d'un scénario idéal pour une élection utilisant la technique du chiffrement homomorphique. ***[VoteHere]***

1. ***Opérations pour initialiser les élections***

   - Les organisateurs des élections initialisent le système par la définition des clefs de déchiffrement des résultats.
     Un ensemble de clefs sera introduit simultanément pour déchiffrer les résultats finaux des élections.
     Les clefs distinctes sont réparties entre différents acteurs ou autorités de confiance.

   - Le bulletin de vote électronique officiel est initialisé et signé de manière digitale.

2. ***Opérations de vote***

   - Chaque électeur demande un bulletin de vote au serveur d'élection après avoir été identifié comme un électeur reconnu et autorisé.

   - Lorsque le bulletin est reçu sur la station de l'électeur, sa validité est vérifiée par la signature électronique.

   - A l'aide d'un logiciel d'interface de vote, l'électeur complète le bulletin de vote électronique

   - Le bulletin de vote ne sera pas retourné vers le serveur mais uniquement le résultat du chiffrement homomorphique des choix effectués par l'électeur.
     En fait le système de vote chiffre des valeurs 1 ou 0 suivant le fait que les cases du bulletin soient cochées ou non par l'électeur.
     La signature électronique de l'électeur couplée au vote chiffré seront retournés vers le serveur de l'organisation des élections.

   - Lors de la réception du vote chiffré par le serveur, la signature permettra d'identifier l'électeur et la validité de son vote (unicité et autorisation de vote).
     Les votes chiffrés acceptés par le système seront directement enregistrés et stockés sur un support mémoire permanent et indélébile (p.e. CD-ROM).
     Un accusé de réception de vote correct, signé de manière digitale par le serveur de vote, sera retourné vers l'électeur.
     Cet accusé ne comporte aucune information sur le vote exprimé par l'électeur.
     Dans le cas où le vote est refusé ou si la signature électronique de l'électeur est erronée, un message d'erreur sera envoyé vers l'électeur.

   - Si l'électeur reçoit un message d'erreur ou s'il ne reçoit aucun message après un temps déterminé, alors il devra recommencer l'opération de vote et ceci jusqu'à la réception de l'accusé de vote correct.

3. Opérations de comptabilisation des votes

- La signature de l'électeur et le vote chiffré sont séparés à l'entrée du système de dépouillement ou de totalisation.

- Les votes chiffrés sont comptabilisés sans être déchiffrés par l'utilisation des propriétés liées au protocole affecté au chiffrement homomorphique.

- En fin d'élection, les organisateurs déchiffrent les résultats finaux par l'introduction simultanée de plusieurs clefs privées de déchiffrement, détenues par plusieurs autorités ou personnes de confiance.
  Il ne sera pas possible de déchiffrer le résultat par l'autorité d'une seule personne.

- Les résultats déchiffrés sont publiés comme les résultats officiels des élections dites de type « papier ».

1.8.5 Arbre des attaques d'un vote électronique

Nous pouvons résumer les agressions possibles sur un vote électronique par la présentation d'un arbre des attaques. ***[VoteHere]***

La représentation d'un arbre des attaques aide à formaliser les menaces de sécurité.

Il montre les assauts qui peuvent être perpétrés sur un système d'élection électronique afin de compromettre les votes exprimés par les électeurs.

Pour récapituler brièvement comment les arbres fonctionnent, chaque niveau décrit une attaque.

D'une façon générale, n'importe quelle intrusion de niveau inférieur réussie, peut être employée pour accomplir une attaque de niveau plus élevé.

Si un système doit résister à n'importe quelle attaque de niveaux supérieurs, alors il doit aussi bien résister à toutes les intrusions de niveaux inférieurs.

Arbre partiel des attaques pour compromettre un vote

1. Modifier un vote

    1.1 Changer le vote sur le serveur

        1.1.1 Convaincre l'opérateur du serveur de changer le vote

        1.1.2 Modifier le vote en utilisant la clé privée de l'électeur

        1.1.3 Pirater le serveur et modifier les fichiers de vote

    1.2 Modifier le vote lors de la transmission sur le réseau

        1.2.1 Envoyer le vote vers un autre serveur

        1.2.2 Intercepter et modifier le message électronique

    1.3 Modifier le vote sur l'ordinateur ou le terminal

        1.3.1 Compromettre le navigateur ou le logiciel de vote

        1.3.2 Supprimer le vote original et envoyer une copie modifiée

        1.3.3 Modifier la vue du bulletin sur l'écran de l'électeur

2. Espionner et consulter un vote

    2.1 Consulter le vote sur le serveur

        2.1.1 Convaincre l'opérateur du serveur pour consulter le vote

        2.1.2 Consulter le vote en utilisant la clé privée de l'électeur

        2.1.3 Consulter le vote au moment de la totalisation (comptage)

        2.1.4 Pirater le serveur et visualiser les fichiers de vote

    2.2 Espionner le vote lors de la transmission sur le réseau

        2.2.1 Contrôler tous les bits du message envoyé

        2.2.2 Intercepter le message chiffré

    2.3 Consulter le vote sur l'ordinateur ou le terminal

        2.3.1 Compromettre le navigateur ou le logiciel de vote

            2.3.1.1 Surveiller en "silence" le choix

            2.3.1.2 Détecter les frappes au clavier ou les zones de pressions sur un écran tactile

        2.3.2 Surveiller physiquement "par-dessus l'épaule" de l'électeur

        2.3.3 Convaincre l'électeur de donner la valeur de son vote

2 Présentation de systèmes de vote (E-Vote)

Les codes électoraux de nos voisins européens prévoient l'usage des machines à voter ou système de vote électronique *E-Vote* non connectés au réseau.
Les machines à voter sont utilisées en Allemagne, aux Pays-Bas, en Suède, en Norvège, au Danemark, et prochainement en Irlande et en Angleterre.

La Belgique a déjà une grande expérience avec son architecture de vote électronique utilisant des cartes magnétiques pour remplacer le traditionnel bulletin de vote papier.

Un autre système de la firme NEDAP est utilisé pour des élections officielles dans plusieurs pays européens comme la Hollande, l'Allemagne et bientôt l'Irlande.
Le système NEDAP est également indépendant d'une connexion à un réseau, mais simplifie encore plus la procédure de vote en "stockant" directement les votes dans la machine à voter.

Il est intéressant de présenter les deux systèmes afin de donner une vue plus complète sur les techniques utilisées pour les élections électronique *E-Vote*.

2.1 Le vote électronique en Belgique.

2.1.1 Historique.

En 1989, le Ministre de l'intérieur, également chargé de la "Modernisation des services publics et des Institutions scientifiques et culturelles nationales", chargea son administration d'examiner les possibilités de substituer au système de vote traditionnel avec bulletins un système de vote faisant appel à des technologies plus modernes. ***[M.I. Elec. 2000]***

L'objectif premier était de parvenir à une simplification et à une modernisation des opérations électorales sans changement radical pour les électeurs.

La nouvelle méthode devait :

- pouvoir être intégrée au système électoral belge (vote obligatoire, proportionnelle et scrutin de listes);
- respecter les lois linguistiques;
- servir pour tous types d'élections existant en Belgique.

Cette étude était motivée par les considérations suivantes :

- il est de plus en plus difficile de trouver suffisamment d'électeurs pour constituer les bureaux de dépouillement;
- le remplacement du bulletin de vote en papier ouvre des perspectives intéressantes, surtout en cas d'élections simultanées et lors d'élections où un grand nombre de sièges est à attribuer (commande de papier, stockage, transport, impression, répartition);
- le grand nombre de listes et de candidats dans certaines circonscriptions électorales rend le dépouillement extrêmement ardu qui s'est d'ailleurs encore compliqué avec la généralisation du vote multiple en 1995;
- la réforme de l'état donne lieu à plusieurs nouvelles élections exigeant plus de bureaux électoraux;
- la population dans son ensemble est de plus en plus confrontée avec des processus automatisés;
- l'extension possible du droit de vote aux étrangers dans le cadre de l'Union européenne;

- la fiabilité et la rapidité accrues du dépouillement.

Ces considérations débouchent sur une attitude positive envers l'électeur et le citoyen :

- plus de recensement manuel mais une totalisation électronique des votes;
- système ergonomique par l'utilisation d'un simple écran d'ordinateur personnel avec un crayon optique et une carte magnétique;
- campagne d'information et sessions d'entraînement dans les communes;
- diffusion rapide de l'ensemble des résultats électoraux auprès de la population;
- coût comparable à celui du vote traditionnel.

Au cours de cette étude, différentes solutions furent examinées et finalement deux systèmes totalement différents furent retenus comme prototypes et testés lors des élections législatives et provinciales de 1991. Les premiers votes automatisés "électroniques" furent organisés dans les cantons électoraux de Waarschoot et de Verlaine.

Dans le premier canton électoral fut testé un panneau électronique tactile reprenant l'équivalent du bulletin de vote (système S.V.I. de Nedap); cette méthode est comparable à celle utilisée aux Pays-Bas depuis des années, où l'électeur exprime son suffrage en poussant sur une touche.
Dans le second canton fut installé un système composé d'une urne électronique et de plusieurs machines à voter (PC) par bureau de vote, l'électeur exprimant son vote sur une carte magnétique à l'aide d'un crayon optique.

Le test de 1991 connut un succès important tant en ce qui concerne l'aspect technique que du point de vue des réactions des électeurs.

En fin de compte, la méthode basée sur l'urne électronique et la carte magnétique fut retenue car à résultats équivalents :

a. le panneau électronique s'avérait difficilement utilisable en cas d'élections simultanées et ne pouvait être utilisé à des fins autres qu'électorales.

b. l'autre système offrait plus de possibilités et de garanties parce que le vote émis était également enregistré sur une carte magnétique individuelle.

c. l'utilisation d'un crayon optique rappelle psychologiquement à l'électeur le crayon rouge traditionnel.

La généralisation progressive du vote automatisé a été permise par la loi du 11 avril 1994.
Celle-ci prévoit qu'un système de vote automatisé comprend :

- une urne électronique;
- des machines à voter;
- des systèmes électroniques de totalisation des votes.

Par arrêté royal délibéré en Conseil des Ministres, il a été décidé que les circonscriptions électorales, les cantons électoraux ou les communes désignés par le Roi seront équipés du vote automatisé pour toutes les élections en Belgique.

Avant d'envisager toute généralisation du système, il fut néanmoins décidé d'organiser un deuxième test dans de grandes circonscriptions où se poseraient non seulement des problèmes techniques ordinaires mais aussi et surtout des problèmes d'organisation. Ce test a eu lieu en 1994 et en 1995 à ANVERS, LIÈGE et BRUXELLES.

Environ 1.400.000 électeurs ont participé aux élections automatisées de 1994 et 1995, soit 20% du corps électoral.

A l'issue d'un appel d'offres, le marché fut attribué à deux constructeurs de sorte que deux systèmes de vote automatisé sont actuellement en usage en Belgique, l'un produit par la firme BULL (système Digivote) et l'autre par le consortium PHILIPS-STESUD (système Jites "Just In Time Electoral System").
A l'avenir, il n'est toutefois pas exclu que d'autres firmes obtiennent l'agrément de nouveaux systèmes pour autant qu'ils satisfassent aux conditions générales d'agrément fixées dans l'arrêté royal du 18 avril 1994 et qu'ils subissent avec succès les tests préalables en matière de sécurité et de fiabilité.

En 1998, il a été décidé d'étendre le vote automatisé à environ 3.250.000 électeurs, ce qui représente environ 44% de l'électorat (7.350.000).

Cette mesure a été appliquée le 13 juin 1999.
Ce jour là, plus de 3 millions d'électeurs dans 201 communes et 62 cantons électoraux ont voté sur un écran dans 4.000 bureaux.

En complément du vote automatisé électronique, un essai a été réalisé au moyen d'un procédé de dépouillement automatisé à lecture optique dans les cantons de Chimay et de Zonnebeke.
Cette formule est principalement axée sur l'automatisation des opérations de recensement des votes.
Le vote même reste manuel et est émis à l'aide d'un crayon sur un bulletin de vote en papier adapté au niveau d'un format A4 standard.
La méthode de dépouillement automatisé par lecture et interprétation optique des bulletins de vote, permet d'accélérer et de simplifier la comptabilisation des résultats.
Un des grands avantages de ce moyen est que les procédures ordinaires de vote restent d'application mais que le nombre de personnes nécessaires pour le dépouillement diminue.
Les mêmes cantons ont utilisé à nouveau la procédure pour les élections du 8 octobre 2000 mais il n'a pas été plus largement déployé.

2.1.2 Description générale du système automatisé

.2.1.2.1 Equipement des bureaux principaux dans des cantons et/ou communes

Au niveau du bureau principal se trouvent une ou plusieurs machines de préparation ou de totalisation, composées d'un ordinateur avec écran, clavier, disque dur et imprimante. ***[M.I. Vote Electronique]***

L'appareil de préparation est utilisée préalablement pour introduire les paramètres des élections (type d'élection, sièges à attribuer, listes de candidats,....) et pour fabriquer les disquettes à destination des bureaux de vote.

Après la fermeture des bureaux de vote, la machine de totalisation du bureau principal, lit les disquettes retournées, totalise les votes qui y sont inscrits et calcule les résultats pour établir le procès-verbal.

.2.1.2.2 Equipement des bureaux de vote

Dans le bureau de vote, se trouvent :

- *Une urne électronique;*
- *En moyenne 5 machines à voter.*

Le minimum légal est fixé à 3 machines à voter par bureau et le maximum est établi à 8.

L'urne électronique est composée d'un ordinateur relié à deux lecteurs de cartes magnétiques :

- un pour la validation des cartes (initialisation);
- un pour l'enregistrement des votes (lecture).

La machine à voter se compose :

- d'un ordinateur équipé d'un écran;
- d'un crayon optique;
- d'un lecteur de cartes magnétiques.

Tous les appareils installés dans le bureau de vote sont autonomes les uns par rapport aux autres.
Un ordinateur peut traiter les votes d'environs 180 électeur par session d'élection.
Un bureau de vote moyen compte environ 900 électeurs.
Les normes sont adaptées en cas d'élections simultanées.

2.1.3 Fiabilité du système et contrôle parlementaire

Voici une liste de neuf mesures appliquées au système de vote automatisé belge en vue de contrôler et garantir la fiabilité. ***[Moniteur Belge]***

1. Avant d'être agréé, un système de vote automatisé doit satisfaire à de nombreux tests.
   Ces essais sont réalisés par le Ministère de l'Intérieur et garantissent que le vote de l'électeur est correctement enregistré et qu'il est fidèlement restitué lors du dépouillement tout en garantissant l'anonymat de l'électeur.

2. Pour chaque élection, les programmes électoraux sont élaborés au Ministère de l'Intérieur. Les codes sont chiffrés et contiennent différentes mesures de sécurité.

3. Les logiciels sont transmis avec les cartes magnétiques individuelles vierges, les supports de mémoires et les codes de sécurité propres à chaque président de bureau, sous enveloppe scellée et contre récépissé aux magistrats-présidents des bureaux électoraux.

4. Les présidents des bureaux effectuent une opération de vote test, appelé "vote de référence", avant l'ouverture de l'élection et ceci sur chaque machine à voter.

5. Le vote de l'électeur est enregistré sur une carte magnétique qui demeure dans l'urne scellée et pourra être relue en cas de problème. La carte magnétique aura été validée dans le bureau au préalable.

6. Un programme de relecture permet à l'électeur de vérifier que le vote qu'il a exprimé est bien conforme à celui enregistré sur la carte.
   Compte tenu du secret du vote, ce logiciel peut difficilement être accessible à d'autres personnes que l'électeur dans les bureaux de votes. Il est toutefois possible aux candidats de s'assurer préalablement de cette conformité.

7. A l'issue du scrutin, une copie de sécurité des informations enregistrées sur le support de mémoire originale de l'urne électronique est effectuée par le président du bureau de vote pour éviter toute contestation et dégradation ultérieure. Les logiciels de vote, les supports magnétiques et les cartes magnétiques individuelles sont conservés jusqu'après la validation et peuvent donc être vérifiés et recomptés si nécessaire.

8. La loi organisant le vote automatisé instaure également un contrôle parlementaire sur les opérations de vote électronique par un "Collège d'Experts" désigné par le parlement fédéral et les parlements des entités fédérées. Ces experts contrôlent l'ensemble des logiciels électoraux, tant au niveau de l'élaboration au Ministère de l'Intérieur qu'au niveau de l'utilisation dans les différents bureaux électoraux. Ce contrôle s'effectue de manière indépendante et dans des bureaux électoraux choisis arbitrairement par les experts. Au terme d'une élection, le Collège des Experts remet un rapport au Ministère de l'Intérieur et à l'assemblée concernée. Celui-ci reprend leurs observations, ainsi que des recommandations et des propositions d'amélioration du vote automatisé.

9. Depuis peu, l'aspect transparence a fait l'objet d'une plus grande attention, en publiant sur le site Internet du Ministère de l'Intérieur les sources des logiciels électoraux. Les codes sources sont conservés dans un coffre bancaire.
   De plus, les compétences du groupe des experts ont été élargies et les tests continuent sur les technologies alternatives comme le scannage et la lecture optique.

2.1.4 Procédure de vote automatisée.

La procédure appliquée dans les bureaux lors du vote automatisé ressemble fort à celle prévue pour le vote traditionnel. ***[M.I. Vote Electronique]***

Les cartes magnétiques remplacent les bulletins de vote.

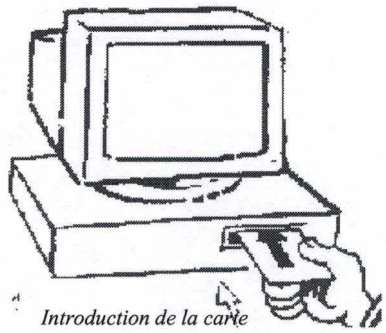
- Après avoir présenté sa carte d'identité et sa convocation, l'électeur reçoit du président du bureau de vote une carte magnétique validée au lieu d'un ou plusieurs bulletins de vote.
- Cette carte est préalablement initialisée par la valideuse dans le bureau de vote, c'est-à-dire rendue opérationnelle pour les élections qui se déroulent ce jour-là dans ce bureau de vote précis. Il sera impossible de voter à l'aide d'une carte validée dans un autre bureau.
- Cette initialisation permet également de donner l'accès, suivant le type d'électeur, à un ou plusieurs bulletins de vote dans le cas des élections simultanées.
- L'électeur se présente dans l'isoloir devant la machine à voter et introduit sa carte magnétique dans le lecteur.
- Les messages à l'écran le guide tout au long de l'opération de vote.
- Il est d'abord demandé à l'électeur de sélectionner la liste de son choix, puis d'exprimer son vote (tête de liste, un ou plusieurs candidats titulaires et/ou suppléants de la même liste).
- Une fois le vote effectué au moyen du crayon optique, l'électeur est invité à confirmer son choix.
- Après confirmation, le vote est définitif et écrit sur la carte magnétique.
- Tant que le vote n'est pas confirmé, l'électeur peut annuler son vote et revenir en arrière.
- L'électeur a également la possibilité de voter "blanc".
- Si l'électeur remet sa carte sans avoir voté, son vote est considéré comme blanc.
- Si plusieurs élections se déroulent simultanément, l'opération décrite se répétera pour chaque élection pour lesquelles l'électeur est autorisé à voter. Les différents votes seront enregistrés sur la même carte magnétique.
- Dans les communes de la Région de Bruxelles-Capitale, dans les communes germanophones et dans certaines communes à facilités linguistiques, l'électeur peut, après introduction de sa carte magnétique, choisir la langue de la procédure de vote.
  La procédure de vote décrite précédemment commence après la confirmation du choix de la langue par l'électeur. Ce choix est définitif pour la durée de la procédure de vote.
- Immédiatement après la confirmation du vote, la carte magnétique ressort du lecteur.
- Une procédure de contrôle et de visualisation des votes exprimés est à la disposition de l'électeur.

A cet effet, l'électeur introduit à nouveau sa carte magnétique dans la fente du lecteur de la machine à voter et l'écran affiche le choix inscrit sur la carte magnétique.
L'électeur ne peut cependant plus rien changer.

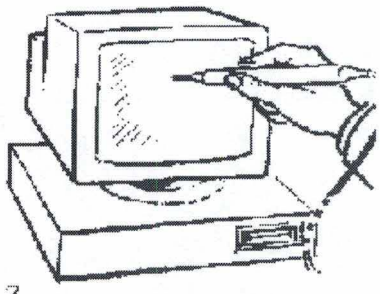
- A l'issue du vote, l'électeur présentera sa carte magnétique au président afin qu'il constate qu'elle ne porte aucune marque.

- La carte est insérée dans le lecteur de l'urne et le vote est enregistré.

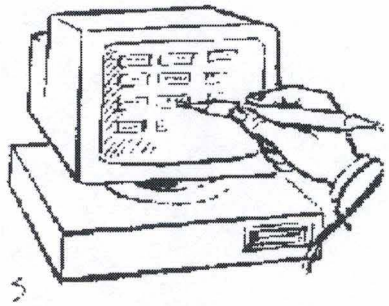
Illustration de la procédure de vote d'un électeur sur une machine à voter.



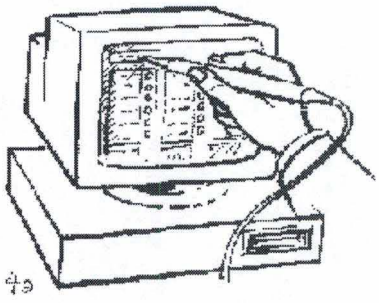
Introduction de la carte



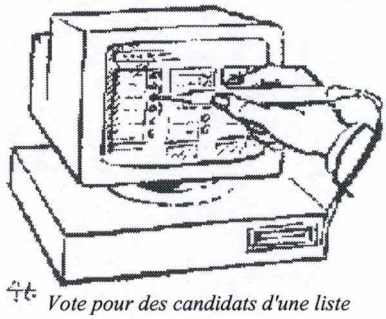
Sélection de la langue



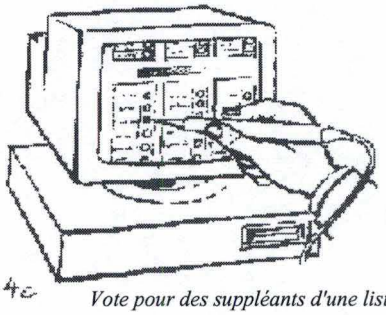
Sélection de la liste ou vote "Blanc"



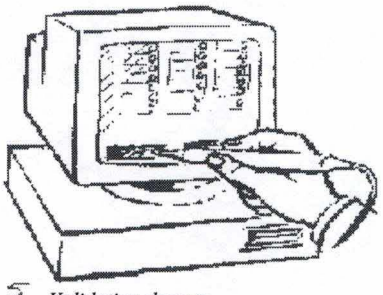
Vote en tête de liste



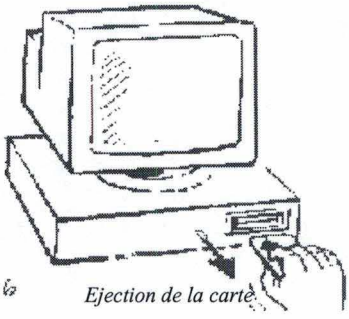
Vote pour des candidats d'une liste



Vote pour des suppléants d'une liste



Validation du vote



Ejection de la carte

2.1.5 Procédures et contrôles du président du bureau de vote

Les présidents des bureaux de votes doivent suivre des directives administratives pour l'organisation et la sécurisation des élections électroniques. ***[M.I. Pres. Bur]***

1. Désignation des assesseurs du bureau de vote
2. Désignation du secrétaire
3. Vérification de l'aménagement du local
    - Chaque machine à voter, installée de manière à ce que le secret de vote ne puisse être violé contient :
        1. Un écran
        2. Une unité PC équipée d'un lecteur de carte magnétique
        3. Un crayon optique
        4. Un système d'alarme (interne ou externe).
    - Le président d'un bureau de vote dispose d'un système qui lui permet :
        1. D'initialiser les cartes magnétiques avant et pendant l'ouverture du bureau.
        2. De stocker les cartes magnétiques après le scrutin.
           L'urne doit, en outre, être équipée d'un bac pouvant être plombé et susceptible de contenir au moins 2.200 cartes magnétiques.
        3. De mémoriser les votes.
        4. De visualiser les compteurs et les différents messages du système.
        5. De communiquer via un clavier.
        6. De clôturer l'élection et totaliser les votes sur un support mémoire électronique.
    - Les cartes magnétiques sont livrées au président du bureau de vote via la commune.
4. Matériel électoral.
    - Etiquettes autocollantes numérotées de 1 à 8 (= le nombre de machines à voter) pour les votes de référence.
    - Colliers Colson noirs, livré aux communes par le Ministère, pour sceller les urnes électroniques ou le sac placé à l'intérieur des urnes.
    - Des enveloppes pour les cartes magnétiques annulées, les cartes magnétiques non utilisées, les votes de référence, la disquette "master", les disquettes backups 1 & 2.

5. Réception des disquettes du logiciel électoral.

   - Avant les élections, le président du bureau reçoit de la part du président du bureau principal de canton, au jour et lieu fixés par celui-ci, contre récépissé, ce qui suit :

     - Une enveloppe scellée et ouatée avec les disquettes du logiciel électoral.

     - Une enveloppe contenant le mot de passe correspondant aux disquettes électorales.

     Remarque : ces enveloppes ne peuvent être ouvertes qu'en présence des membres du bureau. Toute irrégularité doit être mentionnée au procès-verbal.

6. Comptage des cartes magnétiques avant l'ouverture du bureau.

7. Opérations techniques avant l'ouverture du bureau effectuée par le président.

   - Vérifier si le bac de réception de l'urne est vide.

   - Sceller l'urne vide.

   - Démarrer la machine du président.

   - Démarrer toutes les machines à voter dans les isoloirs.

8. Votes de référence.

   - Avant 8h00 et en présence du bureau, le président émet un vote test de référence de la manière suivante :

     a. Il initialise autant de cartes magnétiques qu'il y a de machines à voter.

     b. Il introduit une carte dans la première machine à voter.

     c. Il émet un vote arbitraire à l'aide du crayon optique et note sur le formulaire prévu pour les votes de référence pour quelle liste et pour quel(s) candidat(s) il a voté.

     d. Lorsque la carte magnétique ressort du lecteur, le président y appose une étiquette autocollante sur laquelle est indiqué le numéro de la machine à voter ou de l'isoloir.

     e. Le président recommence la procédure pour chaque machine à voter du bureau avec un seul vote de référence par machine.

   - Une fois que tous les votes de référence ont étés émis, le formulaire est signé par le président et les membres du bureau et placé avec les cartes magnétiques étiquetées dans une enveloppe scellée. Celle-ci est envoyée au président du bureau principal de canton pour un éventuel contrôle.

9. Assistance technique pendant l'élection.

   - Le suivi et la coordination sont assurés par canton et par un fonctionnaire du Ministère de l'Intérieur.

   - L'assistance technique est assurée par le fournisseur du matériel. Celui-ci répare ou remplace le plus vite possible l'appareil défectueux. Toutes les opérations techniques, ouverture d'urne ou annulation de vote, doivent être constatées par les membres du bureau et notées au procès-verbal.

10. Pointage de l'électeur sur la liste officielle.

    - Après présentation de la convocation d'élection et le contrôle de la carte d'identité, l'électeur est "pointé" dans la liste du bureau. Le "pointage" permet de vérifier l'accès au bureau et au vote par l'électeur et également de constater les absences au moment de la clôture des votes.

    - Avec l'accord du président de canton, la commune peut mettre à disposition du président un système de pointage des électeurs à partir d'une liste électronique sur PC à condition d'être en possession d'une liste "papier" des électeurs sur le bureau et d'en vérifier l'exactitude.
      De plus, les coûts éventuels d'un pointage automatisé sont à la charge de la commune et le président du bureau principal porte la responsabilité de la validité du système.

11. Assistance de l'électeur lors du vote automatisé.

    - Le président peut accepter l'assistance envers une personne en difficulté dans une opération de vote automatisé ou encore à une personne handicapée physique. Dans tous les cas, le nom de la personne est indiqué dans le procès-verbal.

12. Procédure de clôture.

    - A partir de 14 h 00, seuls les électeurs présents dans le bureau peuvent encore voter. Le vote est déclaré "clôturé" dès qu'il n'y a plus d'électeurs dans le bâtiment et que tous les membres du bureau ont voté.
      La procédure électronique de clôture et de totalisation des votes dans l'urne doit être activée à partir de la machine du président.

    - Avant 14 h 00, il est nécessaire dresser l'inventaire des cartes magnétiques reprises, des cartes magnétiques non utilisées et la liste des électeurs absents.

    - Après la clôture, les opérations suivantes sont effectuées :

      1. Remplir et signer le procès-verbal

      2. Placer les cartes non-utilisées ou annulées dans une enveloppe spéciale

      3. Idem pour les votes de référence et les différentes disquettes de logiciels électoraux après totalisation de clôture (originale et 2 sauvegardes).

4. Remettre l'urne scellée au responsable désigné par le Collège du Bourgmestre et des Echevins.

5. Les disquettes de logiciel, qui contiennent également les votes des électeurs, sont remises au président du bureau de vote principal du canton et une copie au président du bureau principal communal.

2.1.6 Quelques chiffres

Les cantons qui utilisent un système de vote automatisé représentent environ 44% de l'électorat, soit à peu près 3.250.000 électeurs. ***[M.I. dpt elec]***

- Environ 545.000 dans la région de Bruxelles-Capitale
- Environ 525.000 en Région wallonne (y compris la totalité des électeurs de la Communauté germanophone).
- Environ 2.180.000 en région flamande.

Actuellement, deux sociétés sont agréées pour livrer une solution de vote automatisée en Belgique :

- une société du sud de la Belgique : STESUD SA en association avec Philips (système JITES)
- une société du nord de la Belgique : BULL SA (système DIGIVOTE)

Les deux solutions respectent le "cahier des charges" établi par l'Etat, mais utilisent du matériel différent.

Dans les rapports concernant les élections du 13 juin 1999 et du 8 octobre 2000, le Collège des experts chargés par les Assemblées du contrôle des systèmes de vote et de dépouillement automatisés conclut qu'aucune erreur n'a été constatée et que l'ensemble des contrôles effectués a permis de s'assurer du bon fonctionnement du déroulement du vote électronique. ***[M.I. dpt elec]***

Le pourcentage d'interventions (dépannages) par rapport au nombre de machines à voter électroniques installées était de : ***[M.I. dpt elec]***

Deux Systèmes Belges	**Elections du 13 juin 1999**	**Elections du 8 octobre 2000**
DIGIVOTE de Bull SA	2,7%	1,52%
JITES de Stesud-Philips	1,8%	1,2%

2.1.7 Les quatre objectifs du vote automatisé

Ils sont les suivants : ***[M.I. Elec. 2000]***

1. Les résultats électoraux doivent être rapidement rendus public, non seulement en ce qui concerne la répartition des sièges entre les partis, mais également en ce qui concerne les votes nominatifs de chaque candidat séparément.

2. Le dépouillement des votes doit se dérouler de manière automatisée, au lieu de mobiliser des milliers de personnes le dimanche en journée ainsi que le soir et éventuellement le lundi pour une procédure de dépouillement sans grand intérêt pour les personnes concernées.

3. La procédure de vote doit être simplifiée et rendue conviviale, principalement dans les districts électoraux comptant de multiples listes où les bulletins de vote peuvent atteindre la taille d'un mètre carré.

4. Le coût par vote et par électeur ne peut pas être supérieur à +/- 35 BEF, soit le coût du vote traditionnel, quelle que soit la nouvelle procédure employée.

2.1.8 Comparaisons et détails techniques des systèmes Jites et Digivote.

Deux procédés sont actuellement d'application pour l'organisation des élections électroniques en Belgique. ***[M.I. dpt elec]***

- Le système JITES (Just In Time Electoral System) de STESUD SA.
- Le système DIGIVOTE de BULL SA

Tout en respectant le cahier des charges établi par le Ministère de l'intérieur, les deux solutions présentent quelques différences dans l'implémentation.

Cahier des charges du système d'élection électronique belge

Pour rappel, dans le système d'élection électronique belge, l'électeur peut voter :

a) en tête de liste.
b) pour un ou plusieurs candidats au sein d'une même liste.
c) blanc.

Trois types de machines sont présents dans un bureau de vote : l'URN avec l'URNE et la MAV.

- L'URN est la machine du président du bureau de vote.
- L'URNE est l'urne électronique dans laquelle les cartes magnétiques sont introduites et enregistrées. Celle-ci est liée avec la machine du président (URN).
- La MAV est la machine utilisée par l'électeur dans l'isoloir.

JITES de STESUD	DIGIVOTE de BULL
L'URN et l'URNE forment une seule entité, seulement la valideuse de carte magnétique est externe au système. Les MAV sont différentes et incompatibles avec l'URN. Dans le système JITES, nous ne trouvons donc réellement que deux types de machines dédicacées dans le bureau.	La distinction entre les deux machines ne concerne que le matériel périphérique connecté. La MAV possède un crayon optique et un boîtier d'alarme externe, tandis que l'URN possède un clavier et est connecté à une URNE externe. Chaque MAV peut donc devenir une URN en ajoutant et en retirant du matériel périphérique connecté. L'inverse n'est pas vrai car il est impossible de connecter un crayon optique sur une URN

À l'exception du BIOS [déf. page 39], aucun logiciel n'est installé au départ sur ces machines. Le programme électoral est chargé à partir d'une disquette (rouge – disquette master) qui n'est livrée au président du bureau de vote qu'un ou plusieurs jours avant les élections. Au démarrage, le logiciel vérifie quel est le matériel périphérique connecté et si celui-ci fonctionne correctement. Ce faisant, le logiciel spécifie également le type de machine (MAV ou URN) et indique quel logiciel doit être chargé.

Il existe également deux autres types de machines qui ne sont utilisés que par le Ministère de l'Intérieur ou par les bureaux de totalisation :

- Les machines de préparation des disquettes des logiciels électoraux;
- Les machines de totalisation dans les bureaux centralisateurs.

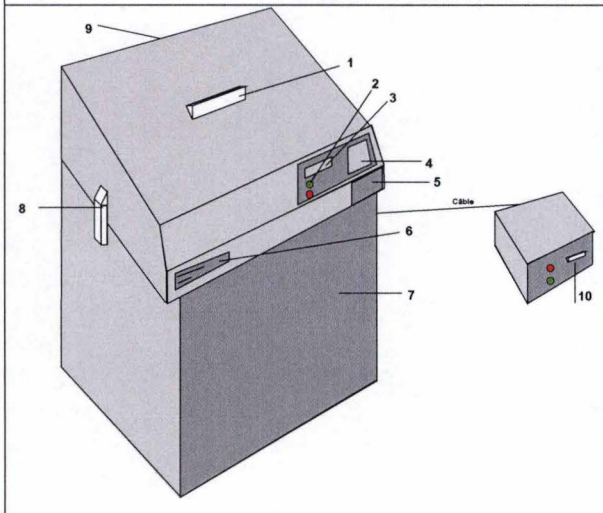
Ces PC sont caractérisés par un disque dur amovible de 105 Mb (SYQUEST) ou par une unité IOMEGA de 100 Mb (ZIP).

Pour le jour des élections, le Président du bureau de vote aura reçu les programmes électoraux :

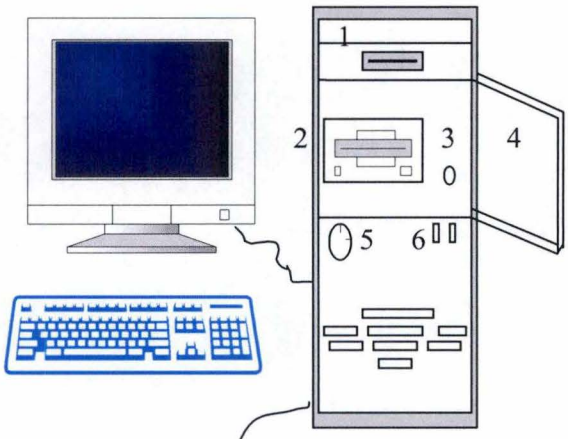
- Trois disquettes pour le démarrage de la machine du président URN (Jites & Digivote) et également pour le démarrage des MAV pour le système Digivote uniquement.
  - 1 disquette de couleur rouge : Master originale
  - 1 disquette de couleur blanche : Master Copie 1 (Backup1)
  - 1 disquette de couleur grise : Master Copie 2 (Backup2)
- Deux disquettes de couleur verte pour le démarrage (original et copie) des MAV pour le système Jites uniquement.

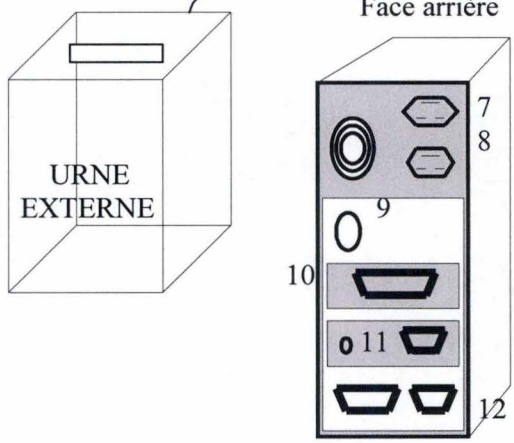
A noter que les disquettes de l'urne (rouge originale et blanche-grises copies) serviront également pour l'enregistrement des résultats contenus dans l'urne lors de la clôture de l'élection.

DISQUETTES	JITES de Stesud	DIGIVOTE de Bull
DEMARRAGE URN	Rouge ou Blanche ou Grise	Rouge ou Blanche ou Grise
DEMARRAGE MAV	Verte n°1 ou n°2	Rouge ou Blanche ou Grise
RESULTAT CLOTURE	Rouge ou Blanche ou Grise	Rouge ou Blanche ou Grise

<table>
<tr><th>JITES de STESUD</th><th>DIGIVOTE de BULL</th></tr>
<tr><td colspan="2">URNE & MACHINE DU PRESIDENT DE BUREAU</td></tr>
<tr><td>


1. un lecteur de bulletins magnétiques
2. des lampes de contrôle
3. un écran de contrôle
4. un clavier numérique
5. un module de mémoire (flash eprom)
6. un lecteur de disquettes
7. un bac de récupération des bulletins magnétiques
8. deux fermetures équipées de plombage
9. une batterie de sauvegarde
10. un boîtier externe pour la valideuse

❶ Ecran LCD
❷ Lampes verte et rouge
❸ Clavier
</td><td>
Face avant


Face arrière


1. un lecteur de bulletins magnétiques
2. un lecteur de disquettes
3. un bouton de mise sous tension et reset
4. une porte de sécurité
5. Serrure de la porte de sécurité
6. Témoin de mise sous tension
7. Alimentation électrique de l'écran
8. Alimentation électrique de la machine
9. Connexion au clavier
10. Connexion à l'écran
11. Connexion à la souris
12. Connexion à l'urne externe
</td></tr>
<tr><td>
L'urne se compose d'une tête et d'un bac. Une valideuse est reliée à l'urne.

<u>La Tête de l'urne se compose extérieurement :</u>
• D'un câble pour l'alimentation électrique de l'urne à partir du secteur. Le câble est fixé à l'urne et il se termine par une fiche,
• D'un lecteur de disquettes avec une
</td><td>
Cette machine est construite à partir d'un PC standard possédant au moins les éléments suivants :

<u>Système digivote I :</u>
- Un boîtier "miditower" permettant l'adaptation d'un lecteur de carte magnétique
- Un PC 386SX, 33Mhz, avec 4Mb de
</td></tr>
</table>

<table>
<tr>
<td>lampe verte,
• Un lecteur de cartes magnétiques,
• Une lampe verte et une lampe rouge,
• Un écran LCD (cristaux liquides),
• Un clavier.
• Un tiroir qui peut recevoir 12 piles.
• La mémorisation protégée contre les pannes de courant des votes durant l'élection à l'aide de la Flash Eprom (côté bureau).

Le Bac de l'urne reçoit les cartes magnétiques (récupération après le vote de l'électeur).

La Valideuse : elle n'est pas raccordée directement au secteur mais par l'intermédiaire du câble venant de l'urne. Elle est constituée principalement :
• D'un lecteur de cartes magnétiques (fente où le président valide la carte magnétique avant de la donner à l'électeur).
• D'une lampe verte et d'une lampe rouge qui décrivent le comportement du lecteur/valideur des cartes magnétiques.</td>
<td>mémoire interne, extensible à 16Mb
- Une carte mère avec une interface "lecteur de disquette /2-ports série et 1 port parallèle"
- Un élément de lecture/écriture de carte magnétique
- Le lecteur de disquette de l'urne
- Un clavier
- Un écran SVG 15'' couleur

<u>Système digivote II :</u>
- Un boîtier "miditower" permettant l'adaptation d'un lecteur de carte magnétique
- Un PC Pentium 233Mhz, avec 8Mb de mémoire interne, extensible à 256Mb
- Une carte mère avec une interface "lecteur de disquette /2-ports série et 1 port parallèle"
- Un élément de lecture/écriture de carte magnétique
- Le lecteur de disquette de l'urne
- Un clavier
- Un écran SVG 15'' couleur

<u>L'URNE électronique externe :</u>

L'urne se compose de deux parties : la partie supérieure, appelée "Tête" et la partie inférieure, appelée "Bac".
La tête de l'urne est connectée à la machine du président.
Le Bac de l'urne reçoit les cartes magnétiques (récupération après le vote de l'électeur).</td>
</tr>
<tr>
<td colspan="2">Après le vote, la carte magnétique est introduite dans une fente qui se situe dans la partie supérieure.
Celle-ci est protégée contre l'introduction d'objets étrangers.
Au moment où la carte magnétique est lue, apparaît à l'écran du PC du président, tant au compteur global, la somme du nombre de cartes déposées dans l'urne. Lors de la validation, le compteur global augmente également d'une unité.</td>
</tr>
</table>

Les votes sont transcrits dans la mémoire Flash Eprom de l'urne et sur la disquette master rouge présente dans le lecteur. Grâce aux batteries de secours, les opérations en cours au niveau de l'urne au moment de la coupure de courant peuvent se terminer. En effet, les batteries permettent de continuer l'élection durant 15 secondes (un message sonore est audible pendant cette période). Ce temps est largement suffisant pour terminer la lecture ou la validation d'une carte. Si durant ce temps, le courant revient, l'urne repart automatiquement. Il convient d'attendre que le courant soit rétabli pour enregistrer les cartes suivantes. Toute carte qui n'est pas tombée dans l'urne n'est pas comptabilisée, il faudra donc la réintroduire.	Les votes sont transcrits sur la disquette master rouge présente dans la machine du président. Pas de protection spéciale contre les coupures de courant mais sécurisation des données par le support physique mémoire (disquette).

Si le système ne permet plus l'écriture des votes sur la disquette Master et sur les copies pendant l'élection, alors le bureau continue en mode "Dégradé".
Dans un tel cas, la clôture ne produira pas de résultat et le bureau principal effectuera une relecture de l'ensemble des cartes magnétiques contenues dans l'urne pour permettre la totalisation des votes et l'édition des résultats.

La fonction de l'URN

L'URN est la machine qui est réservée au président du bureau de vote. Dans le bureau de vote, c'est le seul appareil auquel un clavier ou pavé numérique est connecté. C'est également à cet appareil qu'est raccordée l'urne électronique.

Il n'y a qu'une seule URN par bureau de vote.

Les autres appareils présents dans le bureau de vote sont les machines à voter qui se trouvent dans les isoloirs. Ce genre d'outil situé dans un isoloir s'appelle MAV. Ces appareils ne sont pas dotés de clavier mais un crayon optique et un boîtier d'alarme (interne ou externe) qui avertit de manière visuelle et auditive qu'il se passe quelque chose de fondamentalement anormal au niveau de la machine dans l'isoloir et qu'une intervention est souhaitée.

.

Avec l'URN, le président du bureau de vote exécute :

- l'initialisation de la disquette et de la carte magnétique avec le mot de passe afin de démarrer les machines à voter (=MAV);
- l'initialisation ou la validation des cartes magnétiques pour les électeurs;
- l'acceptation de la carte magnétique et du vote de l'électeur qui y est enregistré;
- le suivi du déroulement des votes.

Par rapport au vote sur papier, l'URN assure l'affichage électronique des bulletins de vote et leur stockage électronique dans l'urne électorale.

L'URN assure également la lecture des cartes magnétiques et des votes qui y sont enregistrés. Les votes lus sont ensuite transcrits sur la disquette master ROUGE et, plus tard dans la journée, totalisés au bureau principal de canton.

Au moment de la fermeture du bureau de vote, les votes sont totalisés et transcrits sur 3 disquettes. La première disquette (rouge) est appelée "MASTER", la seconde (blanche) "BACKUP 1" et la troisième (grise) "BACKUP 2".
Ces backups sont effectués, en premier lieu, afin de sauvegarder les données au cas où "MASTER" serait perdue, volée ou endommagée et en deuxième lieu, pour les totalisations.

JITES de STESUD	**DIGIVOTE de BULL**
Démarrage et utilisation de l'URN	
L'URN possède un interrupteur de mise sous tension, un lecteur de disquette et une touche de remise à zéro qui se trouvent derrière une petite porte fermée. Seul le président du bureau de vote y a accès à l'aide d'une clé. Pour démarrer l'URN placer la disquette "MASTER" ROUGE dans le lecteur et puis allumer le PC à l'aide de l'interrupteur de mise sous tension. Si la disquette "MASTER" semble défectueuse, on peut procéder à un nouveau démarrage à partir de la disquette "BACKUP1". Lorsque la phase de démarrage est terminée, il faut introduire le mot de passe pour démarrer.	
Mot de passe de 5 chiffres	Mot de passe de 8 lettres
L'application initialise une carte magnétique. Le mot de passe est inscrit sur cette carte. Cette carte sera utilisée pour la mise en service des MAV On a droit qu'à trois tentatives au maximum pour introduire le mot de passe correct. Après le troisième énoncé erroné, il y a lieu de recommencer toute la procédure de mise en marche.	
La disquette Master Rouge reste en permanence dans le lecteur du système. Les MAV sont initialisées à partir de la disquette VERTE.	Lorsque toutes les machines MAV sont en service, la disquette est replacée dans le lecteur de disquette de l'URN
Après introduction du mot de passe, le bureau de vote est définitivement ouvert. Durant les élections, l'URN affiche à l'écran un compteur qui indique le nombre de cartes initialisées ou validées et le nombre de cartes déposées dans l'urne électronique. Cela permet de procéder à un suivi permanent du nombre de cartes magnétiques en circulation. Lorsque le bureau de vote est fermé, les fichiers qui contiennent les votes enregistrés, sont clôturés sur la disquette "MASTER"Rouge. Après la transcription, l'URN demande d'introduire la disquette "BACKUP1" dans le lecteur afin d'y faire une copie de sécurité des votes et des totaux. Une fois cette copie effectuée, l'URN va demander d'introduire la disquette "BACKUP2". Après cette manipulation, l'URN peut être mise hors service. Pour ce faire, un menu de gestion est à disposition appelé via la touche <ESC>.	

La machine à voter (MAV)

La MAV est l'appareil qui se trouve dans l'isoloir.
On reconnaît la MAV par le fait qu'elle possède un crayon optique et un boîtier d'alarme (interne ou externe) et ne dispose pas de clavier.

Chaque bureau de vote compte au maximum 8 MAV, chacune installée dans leur isoloir respectif.

La MAV effectue les fonctions de base suivantes :

- La lecture de la carte magnétique de l'électeur;
- L'assistance de l'électeur au moyen de messages s'affichant à l'écran;
- L'affichage des différents bulletins de vote électronique stockés;
- L'acceptation et la validation du (des) vote(s) émis par l'électeur;
- Le chiffrement des données de vote;
- La transcription du vote sur la carte magnétique.

Si l'on compare avec les votes sur papier, la MAV assure l'apparition à l'écran des bulletins de vote. Le crayon optique de la MAV remplace le crayon rouge. Au lieu d'indiquer son choix sur le papier, on indique son choix sur l'écran.

La MAV est également équipée d'un boîtier d'alarme. Ce dispositif vous avertit de manière visuelle et auditive qu'il se passe quelque chose de fondamentalement anormal au niveau de la machine dans l'isoloir et qu'une intervention est souhaitée.

L'électeur a uniquement accès au lecteur de carte magnétique, au crayon optique et à l'écran. Le lecteur de disquette, l'interrupteur de mise sous tension et la touche de remise à zéro se situent derrière la petite porte fermée. Le boîtier d'alarme se trouve à l'extérieur de l'isoloir visible de l'extérieur. Le boîtier d'alarme n'est utilisé que par le président. Lorsqu'un signal visuel et auditif se déclenche, il faut interpréter les messages affichés à l'écran de la MAV et prendre les mesures nécessaires pour remédier à l'erreur. Sur le boîtier d'alarme se trouve un bouton-poussoir qui permet d'interrompre le signal auditif. Lorsque la lampe rouge ou verte s'éteint, l'erreur est réparée.

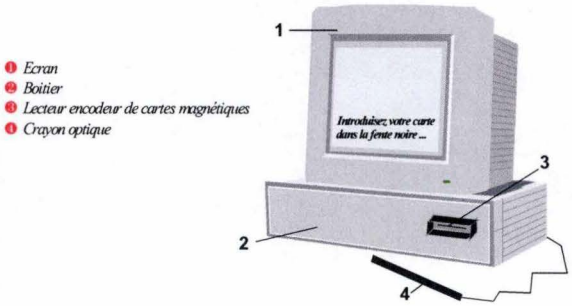
Lorsque que l'électeur a émis son vote, toutes les informations de vote sont effacées de la MAV. Lors de la fermeture du bureau, il suffit d'éteindre l'appareil.

L'utilisation du crayon optique demande quelques mises au point :

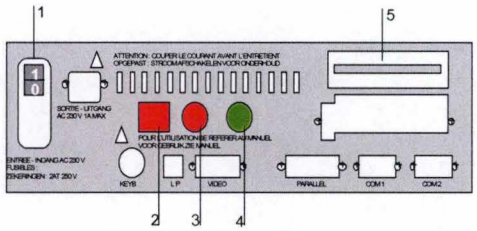
- L'écran doit posséder une intensité suffisante. Le réglage de l'écran a déjà été effectué au préalable.
- Aucune poussière ne peut se trouver sur la pointe du crayon.
- Le crayon doit être tenu perpendiculairement à l'écran.
- Indiquer la case à l'écran ne suffit pas, il est utile d'appuyer de manière sensible contre l'écran.

MACHINE A VOTER

JITES de STESUD

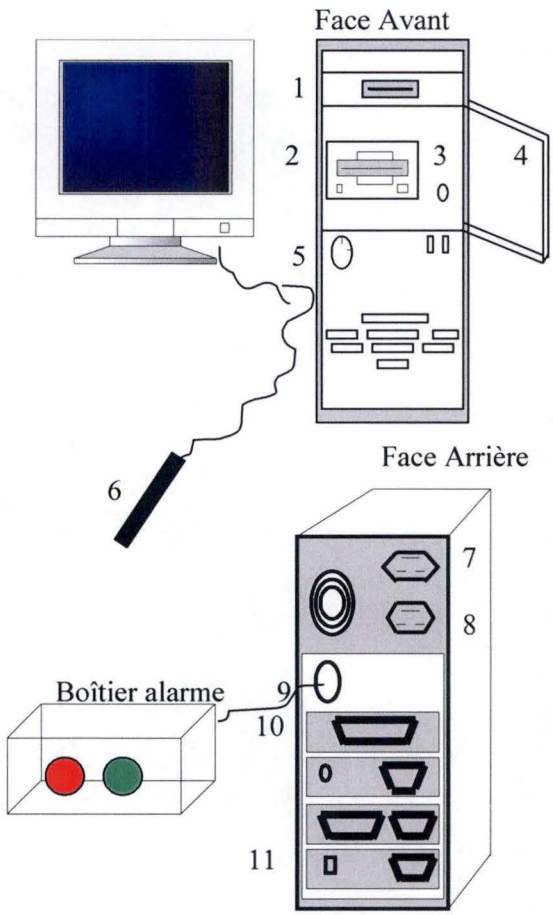


1. *Ecran*
2. *Boitier*
3. *Lecteur encodeur de cartes magnétiques*
4. *Crayon optique*



1. *Interrupteur secteur (1/0 Marche/arrêt)*
2. *Bouton d'interruption du vote*
3. *Lampe rouge*
4. *Lampe verte*
5. *Lecteur de disquettes*

DIGIVOTE de BULL



1. un lecteur de bulletins magnétiques
2. un lecteur de disquettes
3. un bouton de mise sous tension et reset
4. une porte de sécurité
5. Serrure de la porte de sécurité
6. Témoin de mise sous tension
7. Alimentation électrique de l'écran
8. Alimentation électrique de la machine
9. Connexion boîtier Alarme externe
10. Connexion à l'écran
11. Connexion du crayon optique

<table>
<tr>
<td>La MAV se compose d'un ordinateur (boîte plate en fer) qui contient :

<u>Sur sa face avant (visible de l'électeur)</u> :
• Un lecteur de cartes magnétiques.

<u>Sur sa face arrière (visible du bureau)</u> :
• Un interrupteur pour la mise sous tension de l'appareil (ancienne MAV).
• Les nouvelles MAV ne disposent plus d'un interrupteur, et la mise sous tension se réalise en plaçant la fiche dans la prise de courant.
• Un lecteur de disquettes.
• Une lampe verte et une lampe rouge pour signaler les incidents au bureau.
• Un bouton rouge pour débloquer les cartes magnétiques.
• Quatre connecteurs (crayon optique, écran, alimentation électrique machine et écran).
• Un écran de visualisation.
• Un crayon optique.</td>
<td>Cette machine MAV est également construite à partir d'un PC standard possédant au moins les éléments suivants :

• <u>Système digivote I :</u>
Un PC 386SX, 33Mhz, avec 4Mb de mémoire interne, extensible à 16Mb

• <u>Système digivote II :</u>
Un PC Pentium 233Mhz, avec 8Mb de mémoire interne, extensible à 256Mb

• Un boîtier "miditower" permettant l'adaptation d'un lecteur de carte magnétique
• Une carte mère avec une interface "lecteur de disquette /2-ports série et 1 port parallèle"
• Un élément de lecture/écriture de carte magnétique
• Le lecteur de disquette de l'urne
• Un crayon optique
• Un boîtier d'alarme
• Un écran SVG 15'' couleur</td>
</tr>
<tr>
<td colspan="2">Aucune unité de stockage mémoire auxiliaire dans les MAV telle que Disque Dur, Eprom....
Le programme est uniquement stocké en mémoire vive (RAM) et les votes sont chiffrés et placés directement sur le support "carte magnétique".</td>
</tr>
</table>

<u>Démarrage des machines à voter (= MAV)</u>

La disquette master ROUGE pour le système Digivote et VERTE pour le système Jites sont introduites dans le lecteur de la machine à voter et ensuite le bouton POWER est pressé.

L'ordinateur demande alors d'introduire la carte magnétique avec le mot de passe dans le lecteur. Cette carte magnétique a été générée au moment du démarrage de la machine du président. Cette technique permet l'introduction du mot de passe pour le déchiffrement du programme sur la machine à voter sans devoir connecter un clavier à celle-ci.

Ensuite, le système invite à presser la touche "OK" à l'aide du crayon optique pour démarrer la machine à voter. La carte magnétique et la disquette master doivent être récupérées de la machine à voter. Sur les appareils du système Digivote, la petite porte située sur ceux-ci doit être fermée à clef afin que l'électeur ne puisse atteindre le bouton POWER. Les autres machines à voter sont initialisées de la même manière.

Pour le système Digivote, une fois que toutes les machines à voter sont initialisées, la disquette master ROUGE sera replacée dans le lecteur de la machine du président (URN).

Initialisation des cartes magnétiques

Avant que l'électeur ne vote, le président ou son secrétaire doit tout d'abord valider une carte magnétique.

Après la validation de la carte magnétique, celle-ci ressort automatiquement du lecteur. Le compteur "Cartes Validées" qui se trouve sur l'écran principal augmente d'une unité. La carte validée peut, maintenant, être remise à un électeur qui se rend à son tour dans l'isoloir pour voter.

Cette opération d'initialisation des cartes permet l'attribution de droits de vote différents suivant le type d'élection (communale, européenne,...) et le type d'électeur (belge, ressortissant d'un Etat membre de l'U.E). Elle permet aussi de limiter l'accès aux machines à voter du bureau aux cartes initialisées sur la machine du président du bureau. Il est impossible de voter avec une fausse carte ou une carte officielle mais validée dans un autre bureau.

Clôture du bureau de vote

À 14 h 00, le bureau de vote est fermé au public.

La clôture des MAV est assez simple car il suffit d'appuyer sur le bouton POWER pour l'éteindre.

Lorsque le bureau de vote est fermé, le président sélectionne la fonction copie dans le menu des options de l'URN et introduit le code secret.
Tous les votes totalisés et chiffrés sont transcrits sur la disquette rouge "Master Originale".
Après cette transcription, l'urne réclame l'introduction de la disquette blanche "Master Copie 1" dans le lecteur afin d'y sauvegarder une copie de sécurité des votes et des totaux. La même procédure sera ensuite à reproduire pour la disquette grise "Urne Copie 2". Dans le système Jites, la mémoire Flash Eprom est automatiquement réinitialisée.
Lorsque tous les backups sont effectués, le PC doit être éteint en appuyant sur le bouton POWER.
Si pour quelques raisons qu'elles soient, il est impossible d'écrire sur les disquettes lors de la clôture (Master et copies), alors l'urne et les cartes magnétiques seront comptabilisées par relecture au bureau principale.

Il est impossible de réouvrir le bureau et l'élection après l'opération de clôture.

Les logiciels utilisés

Les logiciels développés par Stesud et Bull se répartissent en 4 domaines :

- Les programmes de préparation qui sont destinés au personnel du Ministère de l'intérieur

- Les programmes pour les bureaux de votes.

    1. Le programme pour l'urne.

    2. Le programme pour la machine à voter.

- Le programme pour les P.C. de totalisation :
  Ce programme permet au bureau principal de canton ou communale, de relire les disquettes des différents bureaux de votes, d'en effectuer la totalisation, d'imprimer le procès-verbal des

résultats et de réaliser une disquette avec l'ensemble des résultats du bureau principal.

- Les programmes utilitaires de vérification :

  1. Un programme qui permet de regénérer un fichier de résultat d'un bureau de vote à partir de la relecture des cartes ou de la lecture de la mémoire Flash Eprom pour le système Jites.

  2. Un logiciel qui autorise la relecture du contenu d'une carte magnétique et d'afficher le résultat sur un écran d'une machine à voter. Ce programme équipe les machines à voter depuis les élections d'octobre 2000 afin d'offrir une possibilité de contrôle directe par l'électeur.
     Le même programme est utilisé pour les contrôles de validité des votes de références en rapport avec le procès-verbal du bureau.

	JITES 1.1 de STESUD	**DIGIVOTE 9.7 de BULL**
	LANGAGES DE PROGRAMMATION	
Programmes de préparation	Clipper 5.0	Delphi & Borland C++ 3.0
Programmes Urne	Microsoft C Ver 6.0	Borland C++ 3.0
Programmes Machine à Voter	Borland Turbo C Ver 2.0	Borland C++ 3.0
Programmes Vérifications	Microsoft C Ver 6.0	Borland C++ 3.0

2.1.9 Critiques et qualités du système belge de votes automatisés

Pour clôturer la présentation du système de vote électronique en application actuellement en Belgique, les critiques et qualités exprimées à son sujet sont également exposées. ***[Pour EVA]***

- **Association "Pour EVA"**

  L'"Association Pour une Ethique du Vote Automatisé" est un groupe de pression qui critique le vote automatisé en Belgique.

  Cette association soumet régulièrement des propositions à nos représentants politiques mais introduit également des recours au Conseil d'Etat ou encore devant différentes instances de justice.

  Tout en ne refusant pas l'informatique en général, les responsables de cette association pensent que :

  1. Le système actuel n'offre pas les garanties les plus élémentaires.
  2. Il est essentiel de s'assurer que l'éthique des scrutins soit respectée.
  3. Il est important de ne pas laisser une élite ou des sociétés privées prendre le contrôle des scrutins.
  4. Aucun accomodement n'est tolérable, ce serait compromettre la démocratie.

  En résumé, cette association œuvre pour arrêter le système d'élection électronique au profit unique d'un système de dépouillement automatisé. Elle affirme que cette solution laisse à l'électeur la maîtrise totale et sans intermédiaire de son bulletin, tout en apportant l'automatisation pour un dépouillement plus rapide.

  Le système de dépouillement à lecture optique est donc totalement accepté par l'association EVA.

  Une critique est aussi apportée par le président de l'association sur le principe du système pour l'organisation d'élections simultanées : *"Lors de scrutins simultanés, un 'marquage électronique' est effectué sur les cartes magnétiques remises aux ressortissants européens non belges pour leur 'interdire' l'accès aux scrutins nationaux. De prime abord, ceci paraît insignifiant mais ce marquage permet d'isoler les bulletins ou cartes électroniques de cette catégorie d'électeurs et permettrait de faire des analyses de leurs tendances électorales. Mais il y a plus grave, puisque la liste électorale permet d'identifier les électeurs à chaque urne électronique et puisque la moyenne des électeurs non belges est d'environ 3 à 4 électeurs par urne électronique, puisque leur carte magnétique est 'retrouvable', vous conviendrez que pour beaucoup d'électeurs de cette catégorie, leur secret de leur vote n'est plus garanti !"* ***[Pour EVA]***

  Suite aux remarques et commentaires de l'Association, le gouvernement a fait modifier le système pour les élections d'octobre 2000, par l'introduction d'une fonction de relecture du contenu de la carte magnétique par l'électeur à la suite de son vote.

- **Critiques et qualités du système belge**

  Plusieurs personnes de notoriété publique ou politique "attaquent" et "critiquent" régulièrement le système d'élection électronique, d'autres le présentent comme un exemple de réussite démocratique et invitent les autres pays européens à suivre l'exemple.

Points négatifs du système	Points positifs du système
Plus de témoins de partis au dépouillement, donc le contrôle démocratique est absent.	Le vote étant toujours effectué dans un bureau, ceci offre toutes les garanties de contrôle par les membres du bureau.
Plus de support papier, donc impossibilité de décompte parallèle.	Le système belge garde le principe de 'bulletin de vote' mais sur un support électronique, c'est-à-dire la carte magnétique. Cette solution propose des possibilités de vérification ou de recomptage après l'élection.
Le vote électronique n'étant pas généralisé, le principe d'égalité n'est plus respecté. Certaines listes disposeront du contrôle traditionnel, d'autres pas.	Le système offre une procédure de vote rapide, simple et stable. Toutes personnes, de tous âges, de tous milieux et de tous états physiques ont la possibilité d'utiliser individuellement et facilement le système de vote.
La procédure du vote de référence n'offre pas une garantie sur la validité du système. Comme un seul vote de référence est imposé sur chaque machine à voter, rien n'est plus facile de programmer la fraude à partir du deuxième vote. Il ne devrait pas avoir de limitation et la meilleure solution serait d'effectuer un nombre de vote de référence 'aléatoire' par station à voter. De plus, le contrôle porte uniquement sur la validité du logiciel installé dans les machines à voter. Il n'y a donc pas de test du programme installé dans l'URNE. Le test des votes de références devrait permettre le contrôle complet du cycle d'un vote dans le bureau, c'est-à-dire de la machine à voter jusqu'à sa comptabilisation dans l'urne.	Le matériel et les logiciels sont certifiés et contrôlés par un collège d'experts avant les élections. Les logiciels sont sécurisés par un accès par code secret au moment de leur installation.
La technologie du crayon optique est dépassée ou pas très précise pour les opérations de vote. Il serait plus intéressant d'utiliser des écrans à toucher ou "tactile".	Le système garanti le secret du vote et l'intimité de l'électeur tout en utilisant une architecture simple. Il est suffisamment paramétrable pour permettre une adaptation de la langue d'affichage ou encore d'autoriser l'accès à différents scrutins pour des types d'électeurs bien précis (initialisation de la carte magnétique).

Points négatifs du système	Points positifs du système
Les procédures de démarrage et clôture des bureaux de votes obligent le président à avoir plus que de simples notions en informatique. La liste des erreurs ou problèmes pouvant survenir pendant l'élection est très importante.	En cas de problème dans le système de vote (disquette inutilisable, erreur de manipulation), il sera toujours possible de continuer les votes et de procéder ensuite à la comptabilisation des cartes en "off line" (mode dégradé).
Le fait de valider les cartes à voter est une opération qui prend du temps et qui peut être génératrice d'erreurs. L'organisation d'élections classiques obligeait les assesseurs à placer un "cachet" sur chaque bulletin papier pour le certifier valable. La validation des cartes à voter est similaire et ainsi n'apporte pas plus de souplesse ou moins de travail pour l'organisation des élections.	La procédure de validation des cartes magnétiques permet d'autoriser un vote, sur une des machines à voter du bureau, uniquement avec une carte initialisée sur la machine du président du bureau même. Il est impossible de voter avec une fausse carte ou une carte officielle mais validée dans un autre bureau. De plus cette carte peut être "marquée" électroniquement pour paramétrer le système d'élection (affichage, langue, scrutins) suivant le type d'électeur et ceci sans toucher au secret de vote.
Le matériel étant spécialisé au niveau des composants électroniques, il est autorisé mais difficile de l'utiliser par les communes à d'autres fins en dehors des périodes d'élections.	La spécialisation du matériel informatique utilisé par les machines à voter et l'urne électronique offrent de grandes garanties de sécurité et luttent contre la fraude. De plus, chaque machine à voter est équipée d'un boîtier d'alarme (interne ou externe) indiquant par un signal sonore toute défectuosité du système ou toute tentative de manipulation non autorisée du matériel par un électeur.
En cas de panne électrique ou matérielle, le bureau risque de ne plus pouvoir donner l'accès aux électeurs pendant une période de temps indéterminée. Cette situation est frustrante pour les électeurs qui doivent alors attendre.	Un service d'aide technique est assuré par les sociétés Stesud et Bull pendant la durée de l'élection. Le pourcentage de machines à problèmes a été minime lors des dernières élections (+/- 1,5%).
L'électeur n'a pas confiance en ce que le système informatique écrit sur la carte magnétique et par conséquent doute du respect de son choix de vote par le système.	Le système est ouvert. Les sources des programmes et l'architecture déployée sont des informations en consultation libre pour le grand publique. L'électeur est informé sur le fonctionnement du système par des articles dans la presse, des affiches, des reportages à la télévision. Une brochure et une cassette vidéo d'information ont même été réalisés par les autorités compétentes.

Points négatifs du système	Points positifs du système
Le risque d'erreurs de programmations ou de manipulations malhonnêtes des codes sources sont toujours possibles. La garantie repose sur la certification d'un comité, composé d'un groupe d'experts, au ministère de l'intérieur. Certains experts jugent les protocoles de chiffrements utilisés, pour la protection de disquettes de programmes, dépassés et facilement contournables.	L'installation des logiciels à partir de disquettes sources chiffrées, certifiées et protégées par un code secret, sur des machines 'propres' (vide) avec la réinitialisation du BIOS, offre une grande garantie sur la validité du code programme s'exécutant sur la machine pendant l'élection. De plus les opérations d'initialisation et d'installation des programmes sur les machines à voter, sont effectuées dans le bureau sous le contrôle du président et de ses adjoints.
L'électeur doit continuer à effectuer les opérations de votes en se déplacant dans un bureau.	Par la simplification des opérations de dépouillement, les bureaux de vote électronique sont ouverts plus longtemps aux électeurs (jusque 14 h 00). De plus, il ne faut plus de personnel pour le dépouillement, car l'opération est directement et automatiquement réalisée à la clôture du bureau de vote. Par conséquent, les résultats sont également très rapidement publiables.

2.1.10 L'introduction du I-vote en Belgique ?

Il existe une proposition de loi complétant la loi du 11 avril 1994 organisant le vote automatisé en vue de permettre le vote automatisé à distance : le " I-vote " Déposée par les sénateurs Alain Destexhe (PRL) et Vincent Van Quickenborne (VU-ID). ***[A.P.P.D.D]***

Document législatif n° 2-410/1 du Sénat de Belgique pour la proposition de loi.

Cette proposition de loi vise à autoriser l'électeur à pouvoir voter via Internet, moyen moderne de communication et de transport des informations.

De récentes expériences de *E-vote* ont montré que c'est peut être le chemin à suivre pour restaurer l'intérêt du citoyen pour la politique. Aux Etats-Unis, les autorités locales de Californie, de l'Iowa, du Minnesota, du New Mexico et de l'état de Washington étudient la possibilité de voter via Internet. En Californie, des groupes de citoyens lancent une campagne de pétition en faveur de la légalisation du vote en ligne. Le ministère de la défense des Etats-Unis a organisé, à l'occasion des élections présidentielles de novembre 2000 une expérience avec des militaires basés à l'étranger. Par la suite, le gouvernement envisage de permettre le *E-vote* pour tous les Américains résidant à l'étranger.

De plus, l'expérience belge de vote électronique est un succès reconnu en Europe. Il existe de nombreux avantages au système, entre autres la rapidité des résultats et des prévisions statistiques ainsi qu'une réduction du nombre d'erreurs humaines.

Toutefois, le vote automatisé électronique est loin d'être parfait car l'on fait toujours la file et il peut donc être amélioré.
Le gouvernement s'est d'ailleurs engagé à le perfectionner.

Le *I-vote* prolonge la démarche innovatrice du vote automatisé d'autant plus que la Belgique possède un réseau de connexions très développé, qui permet à presque toute la population d'être connectée à Internet.

Les avantages

Plusieurs éléments plaident en faveur du *I-vote*.

1. Facilité le vote de l'électeur

En 1891, lors de la révision constitutionnelle instaurant le droit de vote obligatoire, le législateur s'est attelé à mettre en place toute une série d'arrangements pratiques permettant à l'électeur de s'acquitter de son devoir sans que celui-ci représente un trop gros fardeau. C'est ainsi que le vote était prévu le dimanche et qu'une navette était affrétée au transport des personnes les plus isolées.

C'est dans cette optique que les défenseurs d'un projet d'*I-Vote* belge se situent.
Internet est un moyen supplémentaire mis à la disposition du citoyen en vue de réaliser son devoir électoral.
L'électeur pouvant bénéficier de la technologie moderne ne devra plus se rendre au bureau de vote, faire la file, etc.
Il pourra voter depuis l'endroit où il se trouve en Belgique ou à l'étranger.

2. Permettre à des citoyens ayant des difficultés motrices de voter

Certaines personnes se trouvent dans de grosses difficultés lorsqu'il s'agit de se déplacer.
Les problèmes de mobilité et d'accessibilité à certains endroits sont une réalité pour les personnes en chaise roulante par exemple, mais également pour toute personne ayant des difficultés motrices.

C'est pourquoi, le *I-vote* permettrait à ces citoyens de voter de chez eux ou de n'importe quelle institution hospitalière ou de soins.
Dans le système actuel, un nombre significatif de personnes hospitalisées ou handicapées ne disposent pas de la possibilité de se rendre à la commune alors qu'elles sont parfaitement aptes à exprimer un choix politique.

Le *I-vote* leur permet de participer à la vie publique et de ne pas faire l'objet d'une discrimination à cette occasion.

3. Lutter contre l'absentéisme électoral

En Belgique, le vote est obligatoire. En théorie, toute personne ne se rendant pas aux urnes est sanctionnée pour son absence au bureau de vote, sauf justification.
Lors des élections de juin 1999, le taux d'absentéisme au niveau du Parlement fédéral était de 9,4%, (soit 691.454 personnes) ce qui est considérable pour un pays où le vote est obligatoire. C'est ce qui fait dirent à certains que le " parti abstentionniste " est d'or et déjà un des principaux partis politiques du pays.

Si certains citoyens se désintéressent ouvertement de *"la chose publique"*, d'autres doivent se rendre à l'étranger pour des raisons professionnelles ou ne souhaitent pas rester dans leur commune par une belle journée ensoleillée par exemple.
Le *I-vote* permettrait de faciliter la mobilisation électorale et apporterait l'absence de discrimination.

4. L'absence de discrimination

Un des arguments avancés dans d'autres démocraties, notamment aux Etats-Unis, pour ne pas mettre en application le *I-vote* est le risque de discrimination vis-à-vis de ceux qui ne maîtrisent pas les nouvelles technologies.
Aux Etats-Unis, où le vote n'est pas obligatoire, le taux de participation aux élections est extrêmement faible, parfois inférieur à 50%.
On constate que c'est parmi les couches défavorisées, aux faibles revenus et en particulier chez les populations noires que le taux de participation est le plus bas.
Rendre le *I-vote* possible risque d'augmenter la participation parmi les couches socio-économiques favorisées et de rendre les élus un peu moins représentatifs de la population prise dans son ensemble.
Il s'agit d'un argument pertinent lorsque le vote n'est pas obligatoire, ce qui n'est pas le cas en Belgique.

5. Le vote des belges résidant à l'étranger

Les personnes expatriées trouveraient dans le *E-vote* la meilleure solution pour pouvoir remplir leur devoir civique sans devoir passer par une série de démarches longues et aujourd'hui coûteuses (le gouvernement s'est engagé à les rendre gratuites). Le *I-vote* pourrait s'effectuer soit directement depuis n'importe quel ordinateur, soit depuis une machine installée dans un consulat ou une ambassade.

Pour l'Etat, ce moyen est plus pratique et plus économique que n'importe quelle autre solution (procuration, organisation de bureaux de vote dans les ambassades, etc.).

6. La facilité de traitement

Les données ainsi récoltées via Internet seront plus facilement traitables et rentreront dans une gestion rapide des votes.

Les mêmes avantages s'y retrouverons que pour le vote automatisé :

- suppression du dépouillement;
- coût inférieur;
- plus grande rapidité pour la divulgation des résultats.

7. Développer l'usage de l'Internet

Développer l'usage d'Internet en Belgique devrait être une priorité nationale compte tenu des enjeux pour l'économie et l'emploi. Permettre le *I-vote* par ce canal est un signal parmi d'autres afin de réaliser cet objectif.

On peut même supposer que le citoyen qui choisirait ce type de vote irait visiter les sites des principaux partis politiques et pourrait disposer d'une information plus riche tant sur le plan quantitatif que qualitatif.

Les problèmes potentiels

L'article 62 de la Constitution stipule que : " (...) le vote est obligatoire et secret. Il a lieu à la commune, sauf les exceptions à déterminer par la loi ".
Ces principes sont davantage développés dans le code électoral du 12 avril 1894. Le vote via Internet peut poser deux types de problèmes :

- En premier lieu, selon la Constitution et l'article 4 du code électoral le vote doit avoir lieu à la commune où l'électeur est inscrit sur les listes électorales. Le principe du vote à la commune est une conséquence du suffrage universel. Avant la révision constitutionnelle de 1893, le vote se déroulait au chef-lieu de l'arrondissement administratif où l'électeur avait son domicile. Il en résultait de nombreux inconvénients. En prévoyant que le législateur peut déroger au principe du vote à la commune, le Constituant songeait à la situation des petites communes.

- Par ailleurs, la loi du 8 juillet 1970 avait prévu trois modalités de vote n'impliquant pas le vote à la commune : le vote par procuration, le vote à l'armée et le vote par correspondance. A l'expérience, il était apparu que le vote à l'armée soulevait des difficultés pratiques tandis que le vote par correspondance donnait lieu à des nombreux abus. La loi du 5 juillet 1976 a réformé le système en supprimant ces deux votes, en adaptant et en étendant le vote par procuration (Titre IV, Chapitre IIIbis du Code électoral). En outre, l'article 89bis du code électoral stipule que les électeurs des communes de Fourons et de Comines-Warneton ont la possibilité de se rendre respectivement à Aubel et à Heuvelland pour voter.

La présente proposition de loi prévoit une exception supplémentaire qui permettrait de voter à partir d'un ordinateur quel que soit l'endroit où l'électeur se trouve.

La règle du vote secret n'a été introduite dans la Constitution qu'en 1921. Auparavant, elle était inscrite dans la loi électorale.

Au siècle dernier, les fraudes électorales étaient innombrables. Les grandes règles pour prévenir les fraudes viennent de la loi du 9 juillet 1877.

Dans chaque bureau de vote sont aménagés des compartiments à l'intérieur desquels les électeurs expriment leur vote. Au moins un compartiment isoloir est prévu par cent cinquante électeurs. L'électeur reçoit des mains du président et pour chaque Chambre législative, s'il y a lieu, un bulletin plié en quatre et estampillé d'un timbre. Il se rend directement dans un des compartiments et y formule son vote.
Une fois que le vote a été exprimé, l'électeur montre au président le bulletin replié et dépose ce dernier dans l'urne.

La question du secret, des pressions et intimidations éventuelles ne se posent plus de la même façon que lorsque le suffrage universel a été instauré. La population belge a acquis une très grande maturité et accepte le principe de la liberté de vote, même au sein d'une même famille.

Dans l'immense majorité des cas, le vote par courrier électronique s'exerçant à domicile ou ailleurs se déroulerait en toute liberté et ne pourrait pas influencer le résultat du vote. Il n'en reste pas moins vrai que dans un faible nombre de cas, le risque, même minime, existe.

Mais la " théorie de l'isoloir " où le secret absolu du vote est respecté est plutôt un mythe. En réalité, en se rendant à l'isoloir, l'électeur peut être influencé de multiples façons par exemple, sur le chemin du bureau de vote ou dans les files d'attente.

Afin d'obtenir une garantie supplémentaire, il serait judicieux d'éventuellement prévoir que la loi précise que l'électeur doit être seul au moment de voter.

Entre autres, l'article 183 du code électoral qui stipule " *sera puni d'un emprisonnement de huit jours à un mois et d'une amende de cinquante à cinq cents francs, ou d'une de ces peines seulement, quiconque, pour déterminer un électeur à s'abstenir de voter ou pour influencer son vote, aura usé à égard de voies de fait, de violences ou de menaces, ou lui aura fait craindre de perdre son emploi ou d'exposer à un dommage sa personne, sa famille ou sa fortune.* " présente des garanties suffisantes.
Notons enfin, que plusieurs pays démocratiques acceptent le principe du secret non absolu au moment du vote; c'est le cas de tous les pays où le vote par correspondance est possible, la France et l'Espagne, par exemple.

Un à priori favorable existe quant au respect de la règle du secret du vote au moment où celui-ci est émis.

Afin de tester l'efficacité du système du vote par Internet, il pourrait être, dans un premier temps, instauré dans quelques arrondissements électoraux avant d'être généralisé. Une méthode similaire avait été utilisée pour le vote automatisé dans les cantons électoraux de Verlaine (Province de Liège) et de Waarschoot (Province de Flandre orientale).

Les aspects techniques

La technologie, basée sur l'utilisation de protocoles Internet standard largement disponibles sur le marché, permet d'assurer :

- La validité du vote au niveau sécurité.
- Confidentialité et contrôle de la donnée transmise.
- Le caractère démocratique du vote, c'est-à-dire que l'électeur est bien unique et est bien celui qu'il prétend, ainsi que l'unicité du vote.
- L'aspect confidentiel du vote : personne ne peut intercepter une session de vote c'est-à-dire la transmission du message au moment du vote (mode transactionnel).
- Il n'est pas possible de "prendre en otage" (hijacking) les sessions, ce qui permet d'éviter les attaques des éventuels " hackers ".
- L'audit du vote, c'est-à-dire la possibilité d'effectuer des contrôles et des vérifications, par exemple de vérifier que le nombre de votes émis et le nombre de votants est bien le même.

Les sénateurs Alain Destexhe (PRL) et Vincent Van Quickenborne (VU-ID) proposent, en pratique, la mise en place du dispositif suivant :

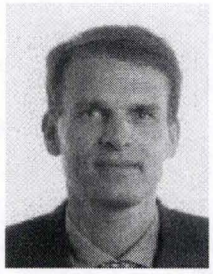
- Sur la convocation de l'électeur figure un code d'autorisation qui est envoyé de la même façon que les codes secrets des cartes bancaires et qui permettrait l'identification électronique.
- De plus, une fois le code utilisé, personne ne pourrait l'utiliser à nouveau pour voter une deuxième fois.
- L'électeur se connecterait sur le serveur et entrerait son code d'autorisation.
- Celui-ci donnerait automatiquement accès aux listes de sa commune.
- L'électeur exécuterait son choix et enverrait son vote.
- Comme le vote est secret, un système de chiffrement du nom et du vote qui seraient envoyés dans deux urnes électroniques différentes.
- Dès que l'électeur aurait envoyé son vote, il recevrait sur son écran un message lui signalant que son vote a été valablement reçu.
- Lorsque les données seraient récoltées, elles seraient introduites dans l'ordinateur de totalisation où les votes Internet seraient mélangés aux votes collectés par ordinateur et ce, de manière aléatoire, afin d'éviter toute discrimination possible.
- Les données réunies seraient traitées comme celles reçues via le vote automatisé avec tout ce que cela compte comme avantages :

    1. Délais d'obtention des résultats plus rapide.
    2. Suppression du dépouillement.
    3. Meilleure utilisation et flexibilité de l'information.

Des procédures encore plus sophistiquées sont possibles, telle que l'utilisation de la signature électronique intégrée dans la prochaine carte d'identitée.

2.1.11 Proposition de loi pour les élections I-Vote en Belgique.

Les députés auteurs du projet : ***[Moniteur Belge]***



Alain Destexhe
sénateur élu directement (F)
PRL FDF MCC

Vincent Van Quickenborne.
sénateur élu directement (N)
VU-ID

Sénat de Belgique

SESSION DE 1999-2000

20 AVRIL 2000

Proposition de loi complétant la loi du 11 avril 1994 organisant le vote automatisé en vue de permettre le vote automatisé à distance

Article 1er

La présente loi règle une matière visée à l'article 77 de la Constitution.

Art. 2

Dans la loi du 11 avril 1994 organisant le vote automatisé, modifiée par les lois du 18 décembre 1998 et du 19 mars 1999, les articles 1er à 29 sont repris sous un titre Ier, intitulé "Le vote automatisé à la commune".

Art. 3

La même loi est complétée par un titre II, rédigé comme suit :

"Titre II. - Le vote automatisé à distance.

Art. 30. - Le Roi peut, par arrêté délibéré en Conseil des ministres, décider que, lors des élections législatives, provinciales et communales, et pour le renouvellement des conseils de communauté et de région ainsi que lors des élections pour le renouvellement du Parlement européen, il est fait usage d'un système de vote automatisé à distance.

Art. 31. - Le Roi détermine les modalités du système de vote automatisé à distance, destinées à garantir sa fiabilité et sa sécurité, ainsi que le secret des votes."

2.2 Le système NEDAP-France Election (Hollande, Allemagne et Irlande)

2.2.1 Historique de Nedap-France Election.

Fondé en 1982, la société France Election est spécialisée dans l'organisation et la fourniture de logiciels ou services associés à cette activité. ***[Nedap]***

En 1975, les premières valises à voter sont mises en service aux Pays-Bas par la société Nedap.

En 1982, le ministère de l'Intérieur des Pays-Bas s'équipe du logiciel de centralisation de France Election pour la comptabilisation des scrutins.

En 1989, les premières communes françaises se dotent du logiciel de préparation des élections.

En 1991, en association avec la Société Nedap N.V. (fabricant de machines à voter depuis 1975), une solution intégrale, associant matériel et logiciel, est développée pour répondre au besoin de modernisation de l'outil électoral en Europe.

S.V.I. : le Système de Vote Intégral

Par la prise en charge de certains travaux préparatoires, la fourniture d'outils et de conseils, le produit de France Election-Nedap permet de limiter les conséquences de l'aspect saisonnier des élections.
Le système est agréé aux Pays-Bas et en Allemagne, 487 communes l'utilisent à ce jour en Europe et la plupart se sont dotées de valises à voter.

En conclusion, 487 communes utilisent 8.000 valises à voter en Europe.

2.2.2 Le concept de "La Valise à Voter".

Le concept de la valise à voter date de 1980, avec la mise en place du modèle ES-1 (400 valises ES-1 sont encore en service à ce jour).
Le modèle ES-2 apparaît en 1986, la valise à voter reçoit alors quelques aménagements et améliorations (700 valises ES-2 sont encore en service à ce jour).
Conçu pour répondre aux divers codes électoraux Européens, le modèle ES-3 est apparu en 1994.

Contrairement aux ordinateurs et autres logiciels utilisés à l'époque de leur commercialisation, les modèles ES-1 et ES-2 ne sont pas obsolètes et remplissent toujours leurs tâches avec satisfaction.
France Election / Nedap.

Le code électoral français prévoit l'usage de machines à voter depuis 1970.
Depuis 1997, France Election sollicite le Ministère de l'Intérieur français pour obtenir l'agrément de la solution des valises à voter.

En décembre 1998, le Ministre de l'Intérieur commande une étude et des propositions sur ce sujet. Actuellement, la solution n'est toujours pas agréée en France pour l'organisation d'élections officielles.
Le système est donc déjà utilisé par des communes françaises, mais pas pour l'organisation d'élections officielles.
Par contre, l'Allemagne et la Hollande ont agréé et adopté la solution de "la valise à voter" pour l'organisation de leurs élections officielles.
De plus, l'Irlande vient de choisir ce matériel pour équiper ses 8.000 bureaux pour les prochaines élections en 2003.
En Angleterre, dans le cadre de la modernisation et de la réforme de l'Etat souhaité par le Gouvernement anglais, une campagne d'expérimentation s'est déroulée à l'occasion des Elections Municipales et Cantonales du 04 mai 2000. Les villes qui le désiraient, pouvaient utiliser officiellement des solutions de vote électronique agréées et utilisées dans d'autres pays. Au préalable, elles devaient présenter leur projet au Ministère de l'Intérieur (Home Office UK) afin qu'il puisse en valider la qualité et la faisabilité. Chacune devait faire son rapport sur le déroulement de son expérimentation. Sur les 32 sites équipés par divers fournisseurs, seule la ville de SALFORD utilisant la solution Nedap a émis un compte rendu très favorable sur le matériel et la prestation. ***[Salford City]***
En Belgique, le système S.V.I. a été testé, mais c'est une autre solution basée sur une urne électronique et l'utilisation de carte magnétique qui fut retenue.

2.2.3 Les caractéristiques de "la Valise à Voter"

1. SIMPLICITE

- L'installation s'effectue par les membres du bureau.
- Elle ne nécessite pas de longues formations ou de connaissances particulières.
- Une utilisation qui tombe sous le sens pour l'électeur c'est-à-dire simplement appuyer sur la ou les touches du ou des candidats choisis et valider.
- Tous les candidats ou les listes sont présentés simultanément à l'électeur.

2. RAPIDITE

La Valise à Voter est une solution rapide pour :

- Préparation du scrutin
- Installation
- Vote de l'électeur
- Permet plusieurs scrutins simultanés
- Dépouillement
- Centralisation des résultats
- Démontage

3. ÉCONOMIE

- Disparition du transport, du tri, du stockage, de la manutention, de la maintenance, de l'entretien, pour ce qui concerne les urnes, les isoloirs, les bulletins et les enveloppes.
- Diminution considérable des dépenses d'installation et de transport du matériel électoral. Diminution considérable des heures supplémentaires accumulées lors des élections par le personnel des communes.
- Une économie moyenne estimée à 450 Euro par scrutin / bureau après études.

4. FIABILITE

- 8.000 valises à voter agréées depuis 1975 aux Pays-Bas et en Allemagne.
- Alimentation 220 Volt ou batterie 12 Volt.
- Aucune voix perdue depuis la première mise en place en 1975.
- Supprime les erreurs de rédaction, les bulletins nuls et les fraudes éventuelles, lors du dépouillement.

5. RESPECT DE LA LEGISLATION

Extrait du "CODE ELECTORAL RELATIF AUX MACHINES A VOTER" Français ***[Nedap]***.

Les machines à voter doivent être d'un modèle agréé par arrêté du ministre de l'intérieur et satisfaire aux conditions suivantes:

1. *Comporter un dispositif qui soustrait l'électeur aux regards pendant le vote; (L.n.88-1262 du 30 déc. 1988) - permettre plusieurs élections de type différent le même jour à compter du 1er. janvier 1991.*
2. *Permettre l'enregistrement d'un vote blanc;*
3. *Ne pas permettre l'enregistrement de plus d'un seul suffrage par électeur (L.n.88-1262 du 30 déc. 1988) et par scrutin;*
4. *Totaliser le nombre des votants sur un compteur qui peut être lu pendant les opérations de vote;*
5. *Totaliser les suffrages obtenus par chaque liste ou chaque candidat ainsi que les votes blancs, sur des compteurs qui ne peuvent être lus qu'après la clôture du scrutin;*
6. *Ne pouvoir être utilisées qu'à l'aide de deux clefs différentes, de telle manière que, pendant la durée du scrutin, l'une reste entre les mains du président du bureau de vote et l'autre entre les mains de l'assesseur tiré au sort parmi l'ensemble des assesseurs.*
7. *S'assurer publiquement, avant le commencement du scrutin, que la machine fonctionne normalement et que tous les compteurs sont à la graduation zéro.*
8. *Le Président, à la fin des opérations de vote, rend visible les compteurs totalisant les suffrages obtenus par chaque liste ou chaque candidat ainsi que les votes blancs, de manière à en permettre la lecture par les membres du bureau, les délégués des candidats et les électeurs présents.*

2.2.4 Le système de vote intégral S.V.I.

Le système de vote intégral - S.V.I. - se compose :

- du logiciel de préparation des élections;
- de la valise à voter.

A noter que le logiciel peut être utilisé sans valise à voter.
Dans ce cas, la centralisation des résultats s'effectue par saisie manuelle.

Caractéristiques :

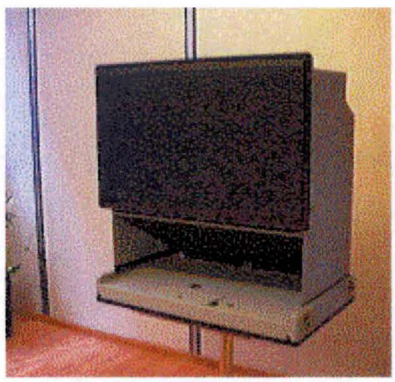
Poids : 26 kg
Taille : 95 x 64 x 18 cm.

Equipée d'une mémoire Flash Eprom, d'une imprimante thermique et d'un écran digital pour affichage des instructions à l'électeur (2 lignes d' affichage).

Table à bulletin programmable, composée de 1.080 touches activables par programmation.

Logiciel d'élection résidant dans l'Eprom, pas de connexion avec d'autres supports de mémoire auxiliaire.

Position fermée



Position ouverte

Conçue pour répondre à de multiples contraintes comme le transport et le stockage.

A l'issue de la préparation du scrutin par le service élection, les valises sont transportées dans les bureaux de vote.

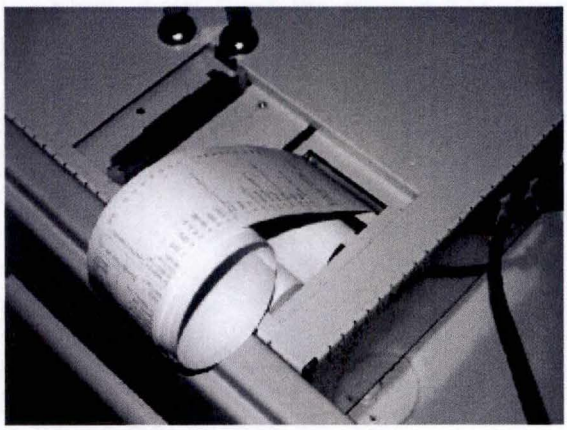
Une valise par bureau et jusqu'à 1.500 électeurs inscrits.

Dans le bureau de vote, le système S.V.I. consiste en un seul et unique élément, c'est-à-dire la "Valise à voter", qu'il suffit de brancher pour rendre le bureau opérationnel.

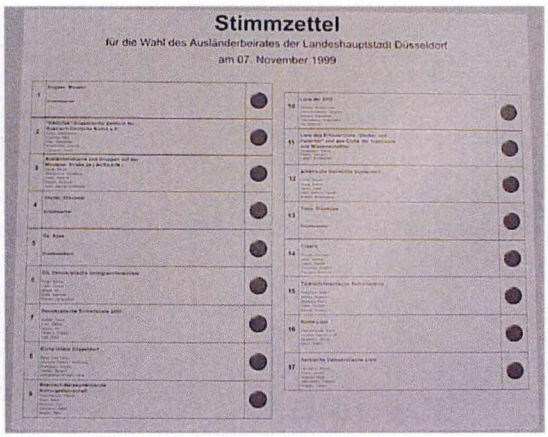
La valise à voter assure plusieurs fonctions simultanément :

- La fonction de la table à bulletin, présentant l'ensemble des candidats ou des listes (jusqu'à 1.080 candidats ou listes)
- La fonction de l'isoloir car l'électeur se trouve seul et à l'abri des regards derrière la valise à voter.
- La fonction de l'urne et de son compteur.

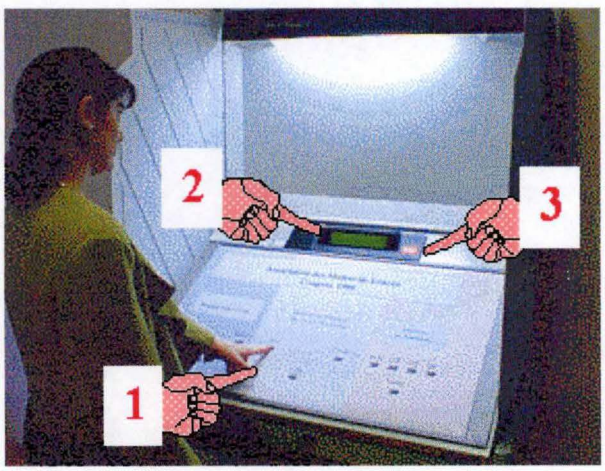
La mise en place de la valise à voter est effectuée par les membres du bureau (prévoir 5 minutes.) Une alimentation par batterie 12 volt est possible pour parer aux problèmes de coupures électriques.



Imprimante intégrée dans la machine pour impression des résultats.



Exemple de bulletin de vote pour la valise à voter.



Exemple de vote d'un électeur :
1. Sélection dans les listes.
2. Bouton pour "CORRECTION" du vote.
3. Bouton pour "VALIDER" le vote

*2.2.5 **Procédure de vote avec le système S.V.I.***

La procédure du vote est très semblable à la méthode classique :

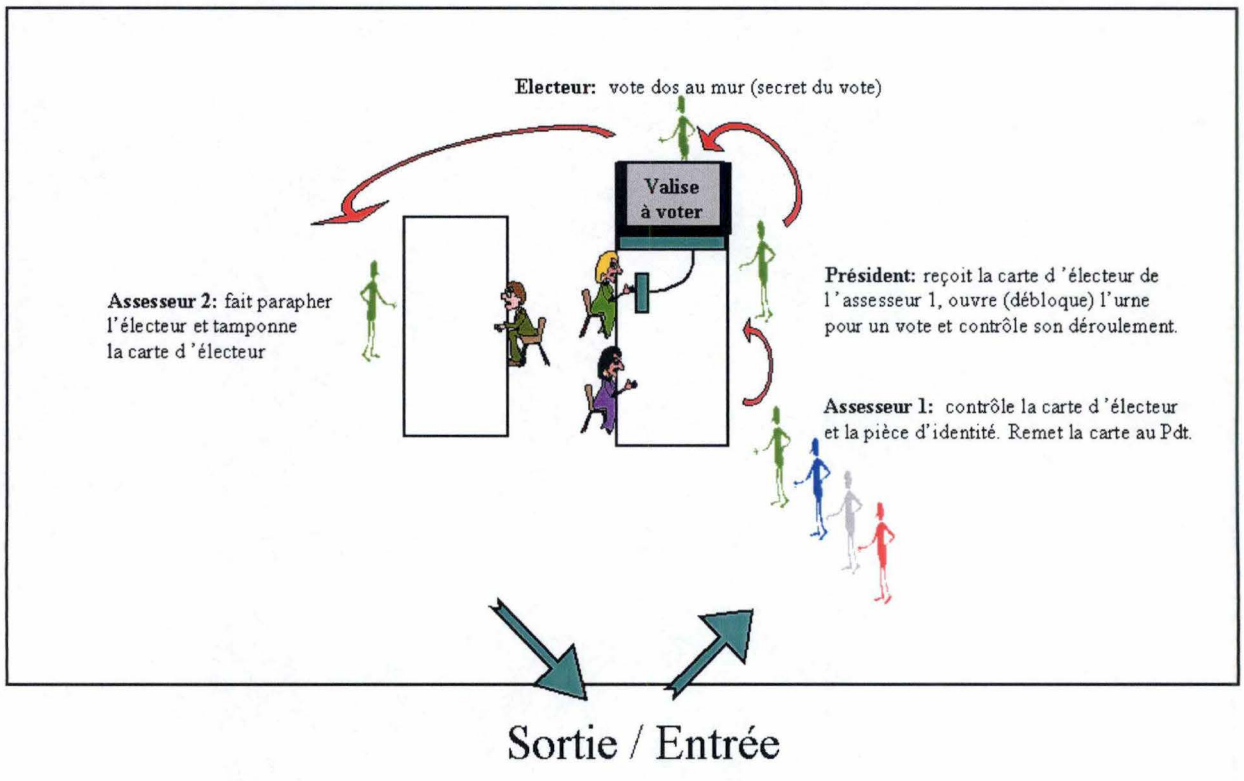
1. L'électeur doit tout d'abord faire contrôler son droit de vote.
   Procédure classique de validation de la carte d'électeur.

2. Le président a, devant lui, un petit boîtier connecté à la machine à voter placée à proximité.
   Il actionne un bouton qui ouvre ou libère électroniquement l'urne, autrement dit donne droit à un vote.

3. L'électeur passe derrière la valise à voter, positionnée de façon à ce que ni ses gestes, ni même son regard puissent être suivis.
   Devant lui, un tableau sur lequel figurent toutes les listes en lice, comme s'il s'agissait de bulletins posés sur une table.
   Sous chacun d'entre eux figure une touche, y compris sous la case "vote blanc".
   Il suffit d'appuyer sur la touche de son choix puis ensuite sur "valider" ou 'corriger" s'il existe une erreur.
   Un petit écran digital informe l'électeur des touches sélectionnées et le guide dans la procédure de vote.

4. A l'issue du vote, après la sélection de la touche "valider", l'urne électronique se bloque d'elle-même dans l'attente du prochain vote autorisé par le Président.
   Le boîtier du président lui signale par un voyant lumineux que le vote est enregistré et il peut donc libérer l'urne pour l'électeur suivant.

5. Enfin, l'électeur signe la liste d'émargement.



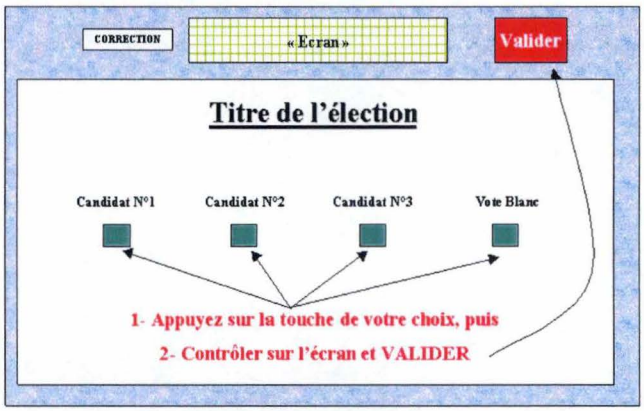
Le déroulement du vote pour l'électeur :

(Bulletin de vote visible par l'électeur)

1. L'électeur effectue son choix en "appuyant" sur le bulletin (Possibilité de vote "Blanc").

2. L'électeur contrôle son choix via l'écran d'affichage digital.

3. L'électeur valide son vote ou corrige son choix.
   Valider le vote correspond au dépôt du bulletin dans l'urne.



- En moyenne, l'opération de vote ne prend que douze secondes par électeur.

- Le vote est enregistré dans la mémoire "morte" (Flash Eprom) de l'urne électronique.
  Le vote ne peut plus être modifié ou se perdre sauf destruction ou vol de l'Eprom.

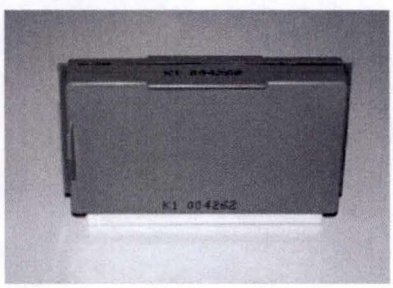
- Après chaque vote, la valise à voter se remet en position fermée ou bloquée.
  Elle ne peut s'ouvrir pour le prochain électeur que par le boîtier de commande du président.

- Comme le demande le code électoral, les valises à voter permettent de réaliser plusieurs scrutins simultanément.

- A la clôture du scrutin, les membres du bureau de vote procèdent au dépouillement à l'aide de l'imprimante intégrée dans la valise à voter.
  En moins de 2 minutes le procès-verbal est prêt, signé et la valise à voter peut être refermée.

Centralisation des résultats :

Le procès-verbal est amené au bureau centralisateur avec l'urne électronique.
Les votes que contient cette dernière dans sa mémoire Flash Eprom, seront centralisés automatiquement à l'aide du logiciel de centralisation S.V.I.

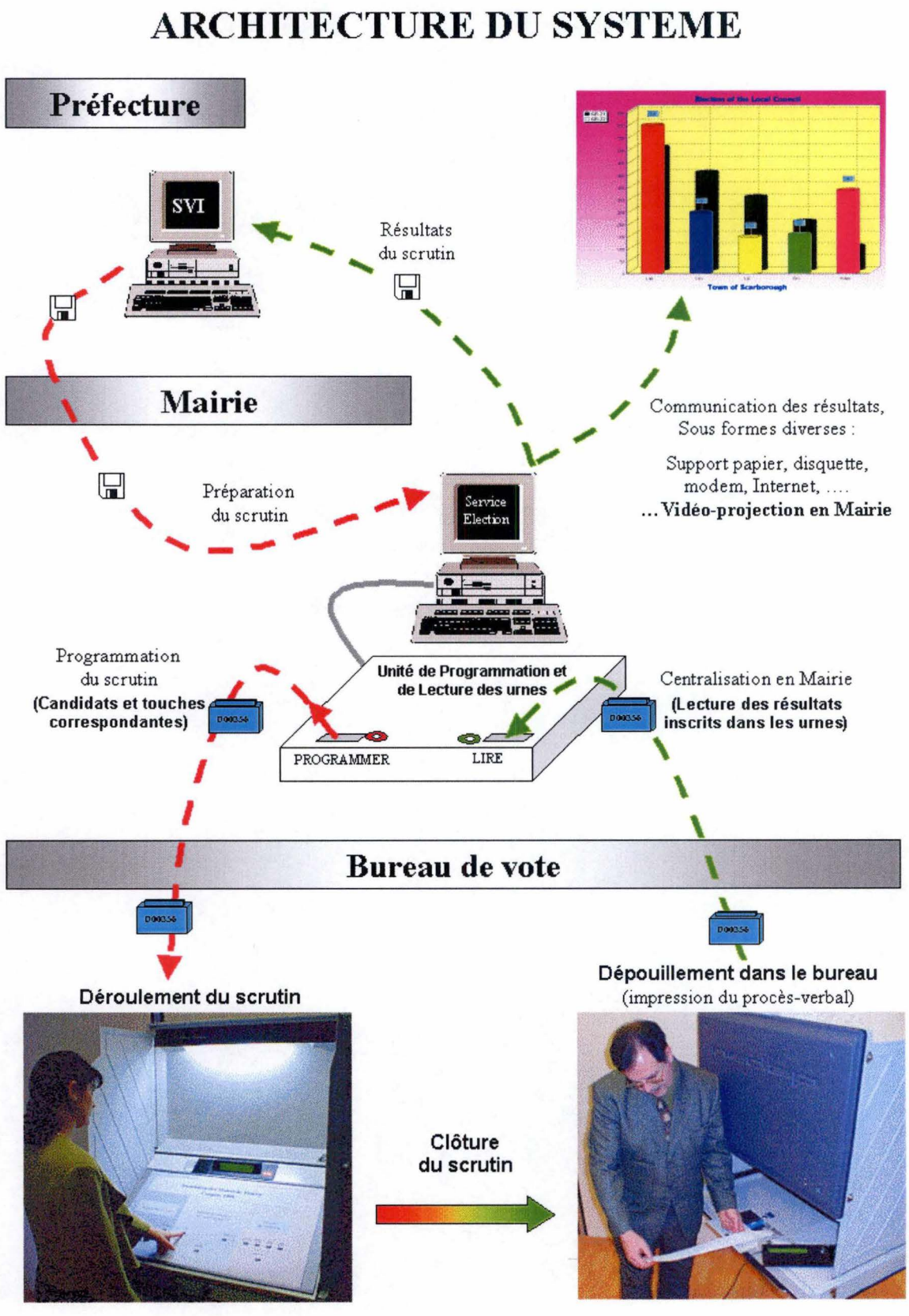


Mémoire Flash Eprom
(Amovible)

Présentation des résultats :

Durant ou à l'issue de la centralisation des résultats, le module Présentation du Système S.V.I. permet de présenter les résultats sous des formes et sur des supports variés (Tableaux, Graphiques, en chiffres et/ou en pourcentages, comparaisons historiques, projection sur téléviseurs ou écran géant …).

2.2.6 *Architecture globale du système S.V.I.*



Les différents logiciels de la solution S.V.I. :

1. Préparation du scrutin :
   - gestion des bureaux de votes et des membres des bureaux de votes (gestion de l'équipement, mailing, sélection, gestion des éventuelles rémunérations ...);
   - préparation du bulletin sur lequel l'ensemble des candidats sont représentés et positionnés;
   - programmation des urnes électroniques;
   - impression des procès-verbaux vierges.

2. Centralisation et présentation des résultats :
   - lecture des résultats contenus dans les urnes électroniques;
   - présentation des résultats provisoires;
   - présentation des résultats définitifs et calcul de la répartition des sièges.

3. Clôture définitive du scrutin :
   - impression des résultats des procès-verbaux du bureau centralisateur;
   - si nécessaire, transfert des résultats vers le ministère sur support informatique.

2.2.7 Critiques et Qualités du système S.V.I. de France Election-Nedap

Clôturons la présentation du système S.V.I. de France Election-Nedap par une analyse critique des points négatifs et positifs de la solution proposée.

Points négatifs du système S.V.I.	Points positifs du système S.V.I.
Il n'y a qu'une valise à voter par bureau prévue dans l'architecture S.V.I. Si plusieurs valises sont installées, il faut multiplier le nombre de boîtiers de contrôle du président et cela complique la procédure de vérification pour savoir si un électeur a bien voter après son passage derrière une des urnes. Il faut donc multiplier le nombre de bureau à machine unique pour éviter un trop grand nombre d'électeur par bureau et des files d'attentes. En cas de panne technique de la machine, l'ensemble du bureau est bloqué.	L'architecture S.V.I. est simple et se limite à une machine à voter par bureau, reliée à un boîtier de contrôle pour le président du bureau. L'installation est rapide et ne demande aucune manipulation "informatique" des membres du bureau. La machine est transportable, autonome en énergie si elle fonctionne sur batteries et d'une utilisation simpliste. L'électeur n'a pas vraiment l'impression de voter sur un ordinateur et donc n'a pas la crainte habituelle du vote sur écran.
L'électeur confie son vote directement à la machine sans possibilité de contrôle. Il lui est impossible de demander une preuve ou une confirmation à postériori de la valeur de son vote stocké dans la mémoire de la machine.	Une procédure de vote simple sans étape "d'interprétation" des bulletins et donc disparition des votes nuls. En une seule opération, l'électeur vote et place son bulletin dans l'urne, c'est-à-dire dans la mémoire de la valise à voter et ceci sans intermédiaire.
Le bureau de contrôle ou de centralisation contrôle uniquement l'égalité des valeurs du procès verbal imprimé par la machine lors de la clôture avec les votes stockés dans la mémoire. En cas de différences, le système ne peut offrir une solution sauf par une règle définie à priori. En cas de destruction de la mémoire Eprom pendant l'élection, il n'y a pas de possibilité de reconstruire l'information des votes perdus.	La valise à voter ne laisse pas la possibilité d'exprimer un vote pouvant être "interprété" ou "modifié" à posteriori.
Le président doit faire confiance à la machine livrée et au logiciel qu'elle comprend. Il n'y a pas de procédure de test ou de vote de référence organisée dans le bureau. La seule preuve est le nombre de votes stockés dans la mémoire de la machine qui est équivalent au nombre d'électeurs qui ont voté.	Le logiciel de vote est "interne" à la machine, dans une mémoire statique et non modifiable. Il a été contrôlé et certifié avant son installation. La société Nedap assiste les autorités dans la réalisation du bulletin de vote et l'adaptation du programme interne à chaque machine.
En dehors de la garantie que la mémoire est vide en début d'élection, aucune autre preuve n'est fournie sur la conformité des choix ou des votes placés dans la mémoire.	Les votes sont stockés sur un support de mémoire statique.

Points négatifs du système S.V.I.	Points positifs du système S.V.I.
En cas d'un nombre élevé de candidats, le bulletin est très chargé et difficilement lisible. De plus, il est difficile d'afficher les listes dans différentes langues car il n'y a qu'un bulletin. Enfin, l'affichage de l'écran digital est très limité et ne peut permettre de solutionner le problème.	La machine "affiche" le bulletin complet pour laisser l'électeur faire son choix. Jusque 1.080 candidats ou listes peuvent être présentés sur le même bulletin.
Malgré la rapidité théorique des opérations de vote, le président doit attendre la fin des opérations pour libérer la machine à un autre électeur, car il n'y a qu'une machine par bureau. Il peut donc rapidement se former des files d'attente lorsqu'un électeur est indécis sur son choix de vote.	Le vote s'accomplit dans l'intimité et le secret, le président est informé lorsque l'électeur a terminé et validé son choix.
En cas de scrutins simultanés, l'ensemble des listes ou candidats pour les différents scrutins, doit prendre place sur un seul espace. La limitation totale reste à 1.080 candidats ou listes pour l'ensemble des scrutins. Il est de plus impossible de paramétrer l'accès ou non de certains électeurs aux différents scrutins. Chaque électeur reçoit les mêmes listes et droits de vote. Le système opère dans un domaine strict et peu paramétrable.	Le système accepte l'organisation de scrutins simultanés lors d'une même élection.
Il existe un risque à confier l'ensemble des développements des outils de gestion, votes et dépouillement dans les mains d'une seule société privée. Ce monopole dans l'organisation de l'élection ouvre la porte au risque de collusion et de fraudes. Les autorités compétentes doivent certifier et vérifier l'ensemble des outils fournis par la société privée avant de les utiliser.	La société Nedap offre une solution logiciel complète avec des programmes de préparations et gestion des élections, des programmes pour les votes sur les machines et des programmes pour la centralisation des votes et la publication des résultats.
Le système est fermé. Les sources des programmes sont des informations secrètes pour le grand publique. De plus la société privée, fournissant le matériel, est largement impliquée dans l'installation et la paramétrisation des logiciels de la machine, car ce type d'intervention est facturé et représente, en grande partie, les recettes de la société.	Le matériel et les logiciels sont certifiés et contrôlés par les autorités compétentes avant les élections. Les logiciels sont sécurisés par une installation "statique" dans une mémoire Eprom de la machine. Ils ne peuvent être changés après installation que par la modification de la mémoire et cette fraude pourra être détectée.

3 Présentation de systèmes de vote connectés à un réseau (I-Vote)

Depuis quelques temps déjà, des solutions d'élections électroniques utilisant des architectures connectées au réseau Internet ou dites "en ligne", sont proposées par des sociétés privées telles que "Election.com", "SafeVote", "VoteHere", "CyberVote", etc.... ***[SecurePoll]***
L'architecture présentée utilise à chaque fois les techniques de chiffrement et de sécurisation de l'information pour répondre aux règles de secret et d'intégrité des votes exprimés.
Jusqu'a présent, seules des initiatives d'élections privées ou des référendums emploient de telles architectures.

Nous sommes peut être arrivés à un tournant important dans l'histoire du vote électronique au travers d'un réseau car, les initiatives se rapprochent de plus en plus du domaine des élections officielles.
De nombreuses études de faisabilités sont entreprises par les gouvernements américains et européens. Des tests portant sur un nombre d'électeurs de plus en plus grand, permettent de juger la fiabilité des solutions proposées.

De grands débats idéologiques sont également initiés pour répondre aux interrogations apportées par le vote électronique à distance telles que :

- Le vote à distance est-il propice aux influences ou aux corruptions d'électeurs ?
- Le vote à distance est-il un remède contre l'abstention ?
- Une nouvelle démocratie : "La cyber-démocratie" ou E-Démocratie.

Par exemple, depuis deux ans, la France organise un "Forum de la démocratie" au mois de mai à Issy-les-Moulineaux. Des "tables rondes" réunissant les spécialistes et acteurs du vote électronique, tant institutionnel que privé, entraînent des discussions sur des sujets comme présentés ci-dessus. ***[Forum démocratie]***

Malgré ces débats, quelques expériences réelles permettent de passer à "l'acte". ***[Elliot]***
Nous présenterons un exemple marquant, c'est-à-dire la première élection publique par Internet ayant une valeur légale: les élections primaires Présidentielles Démocrate en Arizona en mars 2000.

L'Europe suit également le mouvement avec la mise en place du projet E-POLL qui a pour but de fournir un système global de vote électronique pour les élections démocratiques, les rendant plus simples à organiser et plus accessibles aux citoyens. Le système sera testé en 2002 en France et en Italie.

Enfin, la Commission européenne suit avec intérêt le projet "EU-Studentvote" qui, en mars 2002, organisera la première élection en ligne à l'échelle européenne et qui permettra à plusieurs millions d'étudiants d'élire le 'Conseil étudiant européen', qui a vocation à être l'organe de représentation étudiante auprès des institutions européennes. ***[EuStudent]***

3.1 Les élections primaires Présidentielles Démocrates en Arizona

3.1.1 Introduction

La société à capitaux américains "Election.com" est active depuis 25 ans sur le marché de l'organisation d'élections et en a coordonné plus de 600 à ce jour. ***[Election.com]***
La société organise, gère et propose tous types d'élections sur Internet pour toutes élections politiques, privées ainsi que pour les associations sans but lucratif.
L'objectif d'Election.com est de permettre l'augmentation de la participation des électeurs au processus démocratique de leur pays, de leur région, de leurs sociétés ou associations grâce à l'utilisation d'un simple navigateur WEB sur Internet.

Aux Etats-Unis, il est fréquent de confier les tâches d'organisation d'élections à des sociétés privées spécialisées comme "Election.com".
Pour l'organisation des élections primaires Présidentielles du parti Démocrate dans l'état d'Arizona, la société "Election.com" implémenta un système qui offrait 3 options ou possibilités de votes aux électeurs démocrates.

- Option 1 : Le vote classique papier dans un bureau de vote.
- Option 2 : Le vote sur un ordinateur connecté au réseau mais dans un bureau de vote.
- Option 3 : Le vote par Internet à partir de l'ordinateur de l'électeur.

L'élection organisée en mars 2000, a été la première élection ayant valeur légale et utilisant une technique de vote à distance.

3.1.2 Architecture

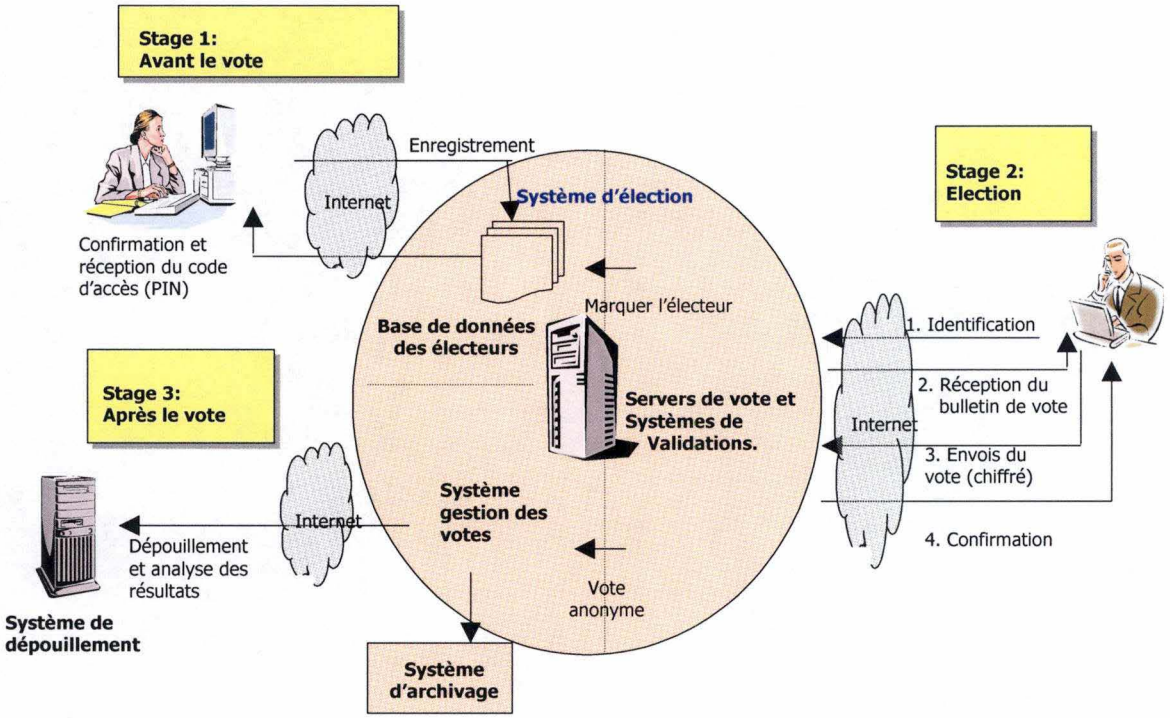
Rappelons qu'une architecture de vote électronique à distance ou par Internet, met en place trois grandes étapes :

1. Les électeurs doivent être enregistrés dans une base de données centralisée et doivent recevoir un code d'accès personnel (Identification et code secret PIN) pour participer à l'élection.

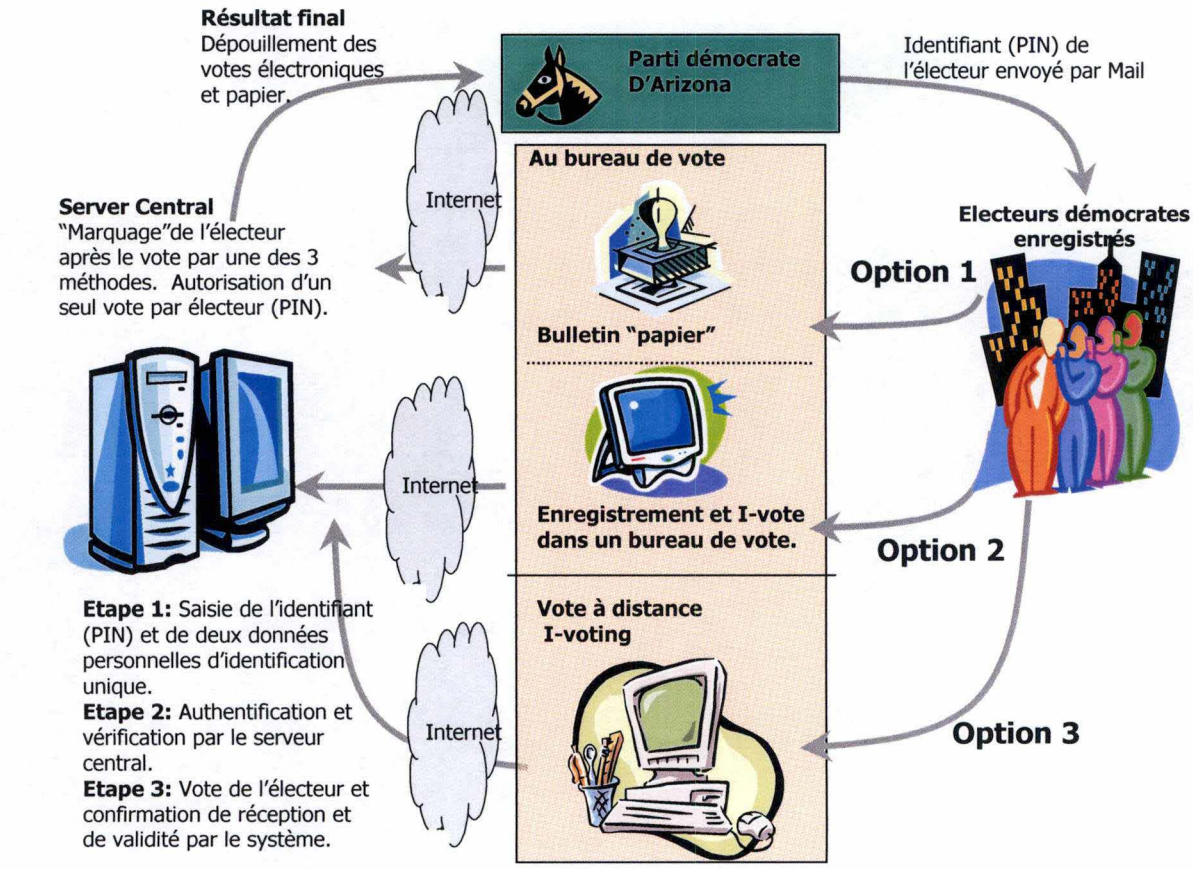
2. Au moment du vote, l'électeur doit être identifié pour lui envoyer un bulletin de vote électronique. L'ordinateur de l'électeur ou la station de vote transmet le vote chiffré aux serveurs de l'élection. Le système d'élection retourne un message de confirmation de bonne réception et de prise en compte du vote.

3. En fin de période d'élection, l'ordinateur de dépouillement comptabilise les votes tout en respectant les règles d'anonymat de l'électeur.

Graphique "Architecture du vote à distance ou par internet" ***[Election.com]***



Graphique "Architecture l'élection Démocrate en Arizona Mars2000" ***[Election.com]***



3.1.3 Déroulement des élections démocrates en Arizona.

L'électeur démocrate de l'état d'Arizona votait pour élire son représentant aux élections présidentielles en mars 2000.
Pour la première fois, le vote était possible soit dans un bureau de vote traditionnel ou électronique, soit à partir d'un ordinateur privé connecté au réseau Internet.

1. Voter par Internet en dehors du bureau de vote :

   Le vote par Internet à partir du domicile de l'électeur ou de tout ordinateur connecté au réseau Internet était permis du mardi 7 mars 2000, 00h01 au vendredi 10 mars 2000, 23 h 59.
   Pour utiliser le vote en ligne de cette façon, les électeurs d'Arizona devaient être inscrits sur les listes électorales en tant que démocrates avant le 24 janvier 2000.
   Le vote à distance était donc autorisé avant l'ouverture des bureaux de votes et pour une période de 4 jours.

2. Voter dans un bureau de vote :

   L'électeur devait se déplacer en personne le jour des élections, le 11 mars 2000 jusqu'à 19h00 dans l'un des 90 bureaux de vote en Arizona.
   Sur place, il pouvait soit voter sur un bulletin en papier traditionnel, soit utiliser les terminaux Internet connectés sur place.

Les électeurs inscrits sur les listes électorales en tant que Démocrate avant le 24 janvier ont reçu par la poste aux alentours du 23 février 2000 leur code d'identification personnel (PIN).
Il était néanmoins possible aux électeurs non inscrits d'utiliser ce procédé le jour de l'élection directement aux bureaux de vote et d'obtenir sur place leur code d'identification pour voter sur un terminal connecté sur place à Internet.

Pour voter à partir d'un ordinateur personnel, celui-ci devait être en possession au minimum d'un accès à Internet et d'un navigateur standard comme Netscape 4.2 ou Microsoft Internet Explorer 4.0.
L'authentification du serveur d'élection et le chiffrement du vote utilisaient la certification de la société VeriSign.

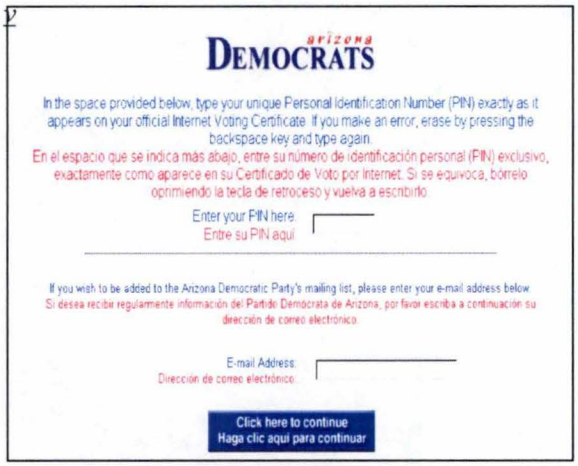
Le système autorise l'électeur à ne voter qu'une seule fois. A cette fin, l'électeur identifié, son code d'accès sera "marqué" et donc inutilisable par la suite.
Le vote par Internet ou via une station de vote dans les bureaux utilise une identification de l'électeur au travers d'une base de données centralisée.
Dans le cas où l'électeur se présente dans un bureau pour voter sur papier, l'employé vérifiera à l'aide d'un terminal, dans la base de données centrale, si l'électeur n'a pas déjà voté par Internet.
Dans le cas où l'électeur serait autorisé à voter sur bulletin papier, l'employé indiquera au système central l'identité de l'électeur pour empêcher un autre vote dans un autre bureau ou un vote en ligne.

L'authentification "en ligne" de l'électeur était basée sur le code personnel qui lui avait été attribué et sur l'introduction de données privées, c'est-à-dire la date de naissance et les 4 derniers chiffres de son numéro de sécurité sociale.

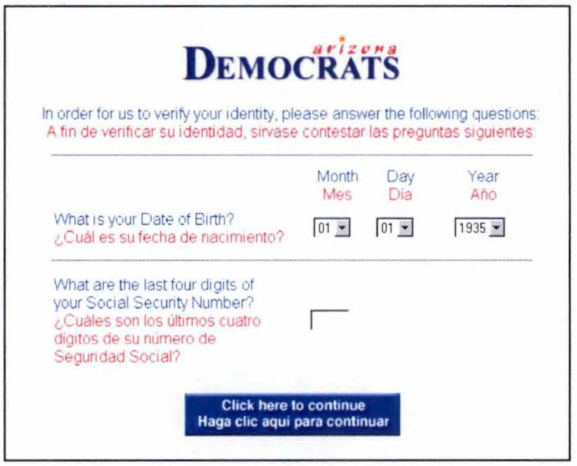
Les systèmes et bases de données informatiques pour d'identification des électeurs, la réception des votes et le dépouillement des résultats sont séparés et indépendants.
Il n'y a donc pas de lien entre l'identité de l'électeur et le vote exprimé.

L'organisation déployée pour l'élection utilisait 6 serveurs pour la réception des votes afin de protéger l'architecture contre les attaques extérieures et la perte d'information.

Exemple scénario d'un vote par Internet à domicile ou sur une station de vote : ***[Election.com]***



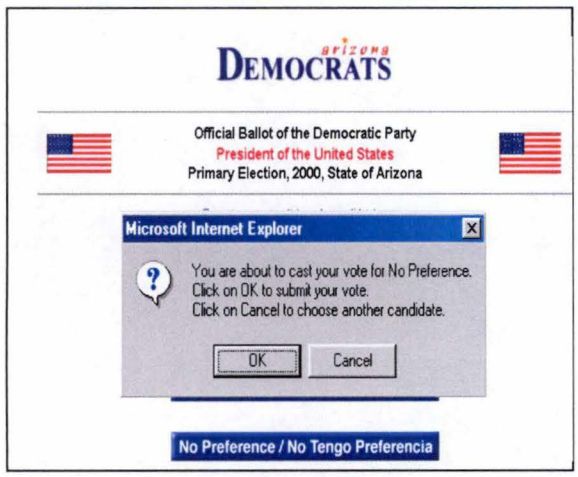
(1) Introduction du code PIN (identifiant de l'électeur)



(2) Introduction de données personnelles

(3) Confirmation de l'identité.

(4) Choix du candidat ou vote "blanc".



(5) Confirmation du choix ou annulation.

(6) Fin de procédure et confirmation du vote.

3.1.4 Conclusions de l'expérience démocrate en Arizona.

Les élections primaires organisées en mars 2000 par le parti démocrate en Arizona ont été une réussite. En effet, le taux de participation était 7 fois supérieure que lors de la précédente élection en 1996 tout en étant de seulement 21%. De plus, il y eut jusqu'à 100% d'augmentation de la participation au sein de minorités Hispaniques et Apaches. Le vote était massif à plus de 70% sur Internet de la tranche des électeurs âgés de 18 à 50 ans.
Sur un total de 85.970 électeurs, 40.000 plébiscites ont voté via Internet et notamment 36.000 à partir d'un ordinateur personnel avant le jour des élections. Ceci nous donne 41% de votes à distance via Internet et 5% de votes sur les stations connectées à Internet dans les bureaux de vote. A l'exception de quelques ralentissements sur le réseau, dus au succès de l'élection, celle-ci s'est déroulée sans problème et la sécurité du système a résisté à toute tentative de piratage. Aux heures de repas, on enregistrait une moyenne de 200 votes par minute. ***[Election.com]***

3.1.5 Synthèse de l'architecture d'Election.com

L'architecture du système d'Election.com utilise de nombreuses mesures de sécurités telles que :

- Un serveur sécurisé d'identification des électeurs;
- Une identification et authentification à l'aide des moyens suivants :
  - une autorisation de vote;
  - un mot de passe pour chaque électeur;
  - des données personnelles obtenues par la liste électorale (date de naissance et numéro de sécurité sociale);
  - un système de chiffrement et de certification pour la transmission des votes par Internet (VeriSign).
- Une séparation complète du vote et de l'identité de l'électeur;
- Un dépouillement des votes et un calcul automatisé des résultats;
- Des outils, des procédures de contrôle et d'audit assurant l'anonymat de l'électeur.

Les électeurs reçoivent leur code d'identification personnel par courrier ou sur les lieux de l'élection. Ils sont alors autorisés à entrer ces informations sur le site sécurisé d'élection. Après validation de ces données en concordance avec l'introduction d'informations personnelles (date de naissance et numéro de sécurité sociale), l'électeur exprime et valide son opinion par simples clics de souris.

Les codes personnels et le vote de l'électeur étant stockés dans deux bases de données différentes, aucun lien ne peut être établi entre l'électeur et son vote.
De même, une fois authentifiés, ces codes ne peuvent être réutilisés, donc un seul vote possible par électeur. Tous les calculs de votes sont comptabilisés par des processus de chiffrement utilisant des codes d'identification (PIN) de 10 caractères et une clef de chiffrement de 128 bits. Actuellement, un ordinateur éprouve des difficultés à casser ces clefs.

Pour les primaires en Arizona, le système a subit 200 tentatives d'assauts et de piratages qui ont toutes échouées. De plus, avant les élections, la société avait informé via Internet et mis à disposition des "pirates" informatique un centre d'élection de test répondant aux mêmes critères technologiques et sécuritaires que le centre officiel. Il a été proposé aux "pirates" de tester et d'essayer toutes les intrusions possibles afin de garantir la solidité du système. Il existe même un forum d'échange d'informations afin de trouver une faille sécuritaire. Malgré la divulgation volontaire d'informations sur la technologie employée, toutes les agressions ont échoué ou ont été détectées. ***[SecurePoll]***

Depuis septembre 2000, la méthode est annoncée plus performante car, actuellement, elle autorise la saisie de 4.000 votes par seconde. Grâce à la plate-forme Datacenter Server Windows 2000 de Microsoft s'appuyant sur la technologie des clusters Compaq, l'application permet à 200 millions d'électeurs de voter sur une période de 15 heures. Ce chiffre correspond à 4.000 votes sécurisés à la seconde.
Le centre informatique des élections utilise un ensemble clustérisé de 42 serveurs frontaux WEB Compaq allié à un système déporté Compaq Proliant ML770 de 32 serveurs. Le Datacenter Server Windows 2000, sur ce nouveau matériel Compaq, permet à Election.com de fiabiliser totalement son application en atteignant le chiffre idéal de 99,999% de disponibilité. ***[Cranor's]***

3.2 Européan EU-Student Vote mars 2002 par Election.com.

Avec l'aide notamment des Facultés Universitaires Notre-Dame de la Paix de Namur, l'élection électronique du premier Conseil européen des étudiants deviendra réalité en mars 2002. ***[EuStudent]***

Prévu initialement pour juin 2001, c'est donc en mars 2002 que l'EU Student Vote deviendra réalité, grâce à la mise en ligne de l'élection du premier Conseil européen des étudiants.
Cette élection sera ouverte à 25 millions d'étudiants européens. Une telle expérience vise principalement à sensibiliser les étudiants aux enjeux, non seulement posés par l'Euro-démocratie et l'Euro-citoyenneté, mais également en relation avec l'enseignement supérieur en Europe.
L'EU-Student devrait fournir une première occasion, à l'échelle européenne, d'analyser scientifiquement l'expérience du vote en ligne et permettra donc tant aux décideurs politiques qu'aux opérateurs technologiques et sociaux d'en tirer des conclusions.

Les Facultés Universitaires Notre Dame de la Paix y participent, et ce de deux manières : par le biais de la cellule de recherche, la CITA (Cellule Interfacultaire de Technology Assessment), et en soutenant l'initiative en mettant à la disposition des étudiants au moment du scrutin des bureaux de vote électroniques. ***[Cita]***

Plusieurs chefs de gouvernement de l'Union européenne et le Premier ministre, Guy Verhofstadt, soutiennent le projet de "Démocratie Electronique".

D'autres Universités, mais également le CNRS, la fondation Robert Schuman, PROMETHEUS-EUROPE, la fondation Hippocrène ... sont partenaires dans l'organisation de cette élection.
Un partenaire privé est également présent, il s'agit de la société ELECTION.COM qui fournira la méthode d'enregistrement "en ligne" et le vote par Internet.
Ce sera donc le même système que celui utilisé pour les élections primaires Démocrates en Arizona. Cette expérience constitue la première étape pour la conquête du vieux continent par la société leader dans l'organisation des élections outre Atlantique.

Qui pourra voter ?

Les étudiants possesseurs d'une carte d'étudiant d'un établissement d'enseignement supérieur de l'Union européenne valide pour l'année universitaire en cours. Les étudiants exprimeront leurs votes à partir de n'importe quel ordinateur connecté à Internet.

Comment s'inscrire sur les listes électorales ?

Au sein de chaque université, les organisateurs des élections ont mis en place des groupes relais de cinq personnes ou étudiants au minimum. Ces relais sont appelés les RA (Registration Authority).
La fonction des RA est d'assurer l'authentification des votants en vérifiant leur carte d'étudiant ainsi que leur carte d'identité officielle avant de les enregistrer dans le système.
Après enregistrement par le RA, un code personnel et un mot de passe seront générés pour chaque étudiant inscrit et envoyés à son e-mail.
Chaque participant à l'opération recevra un code PIN (dix chiffres) et un mot de passe (six chiffres) générés aléatoirement par le logiciel d'Election.com.

Quelle est la procédure de vote ?

Les étudiants pourront voter à partir de n'importe quel ordinateur en toute sécurité et intégrité simplement, en entrant, sur leur navigateur Web l'adresse envoyée par e-mail avec les codes d'identification.
A l'aide du code personnel et du mot de passe, et après authentification par le système de l'introduction de données personnelles (date naissance, numéro carte identité), l'électeur pourra accéder au site web sécurisé d'élection et exprimer son opinion en ligne.

Quels sont les objectifs du nombre d'électeurs ?

Actuellement, l'Europe compte 25 millions d'étudiants et les organisateurs estiment à 15 millions le nombre d'étudiants qui seront informés sur l'élection. ***[EuStudent]***
Néanmoins, une étude considère qu'environ 1 million d'étudiants voteront, ce qui semble peu mais qui est la conséquence de la non obligation de vote.

Une élection semblable, appelée Youth-e-Vote 2000, a été organisée avec les étudiants américains le 7 novembre 2000.
C'est également la société ELECTION.COM qui était l'animatrice et cette élection a rassemblé 1.330.913 électeurs sur un total de 55 millions d'étudiants.
Le Youth-e-Vote 2000 permettait à tous les étudiants âgés de 18 à 24 ans d'élire, une semaine à l'avance par un vote blanc, le président, les sénateurs, les députés et le gouverneur. Les résultats étaient annoncés le jeudi précédant le jour de l'élection officielle en Amérique.
Les étudiants avaient notamment voté à 56% pour la victoire au Présidentielle du Républicain George W. Bush et à 38% pour le Démocrate Al Gore. ***[Election.com]***

.

3.3 Réflexions sur les expériences et projets d'*I-vote.*

Suite à la présentation des grands projets ou expériences de vote en ligne, nous pouvons essayer de répondre à quelques questions en rapport avec le sujet.

3.3.1 La gestion des élections par une société privée.

Il existe une grande différence de culture entre les pays anglo-saxons, où la notion d'outsourcing est parfaitement intégrée et la Belgique. Aux États-Unis et en Grande-Bretagne, les élections, notamment syndicales, sont beaucoup plus nombreuses et obligatoires. Dans un pays aussi vaste que les États-Unis par exemple, la méthode de vote par le papier et gérée par des bénévoles est inconcevable. Les risques d'erreur sont beaucoup trop grands. Le comptage automatique des bulletins de vote est monnaie courante depuis longtemps là-bas et si les élections se professionnalisent, c'est parce que les États voient l'intérêt de travailler avec des sociétés qui n'ont pas de parti pris dans les élections.
Il existe néanmoins des expériences plus malheureuses, par exemple au Vénézuela, sur les conseils d'une multinationale soi-disant spécialisée dans les élections, l'organisation et l'encadrement des dernières élections ne furent pas décentralisés au niveau des collectivités mais complètement pris en charge par cette société privée, au niveau national.
Les conséquences furent catastrophiques. Ce scrutin a été invalidé et les électeurs re-convoqués ultérieurement. L'élection était cette fois-ci préparée comme à l'accoutumé par les collectivités locales.
Il faut également faire attention à l'installation d'un monopole dans le domaine, car il est un fait que la société Election.com est extrêmement active sur le marché et essaye maintenant de conquérir l'Europe en partenariat avec la société française Matra.

3.3.2 Le problème de l'absence d'isoloir pour le vote à domicile.

La question de l'absence d'isoloir ne se pose pas aux Etats-Unis, en Scandinavie, en Allemagne, en Angleterre, en Suisse et aux Pays-Bas.
La raison en est très simple : ces pays ont déjà mis en place le vote par correspondance.
Mais si on réduit l'isoloir au domicile des votants, qui sait ce qu'il pourrait s'y passer?
Faut-il craindre les pressions de l'entourage familial ?
On peut aussi imaginer que la bonne vieille méthode consistant à convoyer avec bienveillance des retraités en minibus jusqu'au bureau de vote céderait la place à un coup de pouce électronique, pour pallier leur ignorance technologique...
En Suisse, on s'est également rendu compte que le libre arbitre était souvent plus grand grâce au vote par correspondance que par le vote dans l'isoloir. Par exemple, un parti très militant obtenait de bons des résultats aux élections parce qu'ils convoyaient, entre autres, les personnes âgées pour les faire voter et de préférence pour eux. Depuis la mise en place du vote par correspondance, ce parti a presque disparu. Et aujourd'hui, en Suisse, seuls 5% des électeurs se rendent dans les bureaux de vote. ***[Cranor's]***
Il ne faut pas être hypocrite sur le pouvoir symbolique de l'isoloir. Ce n'est pas parce qu'on s'enferme deux minutes dans un isoloir qu'on possède son libre-arbitre. Celui-ci est peut-être plus présent quand on est tranquille chez soi et que l'on prend le temps de s'informer avant de choisir. Et Internet ou pas, il existera toujours des gens sous influence.

3.4 Projets financés par la Commission Européenne.

A Bruxelles, la Commission apporte son soutien et subventionne plusieurs projets d'origine européenne dans le cadre de l'appel d'offres IST (Information Society Technology).
En dehors des solutions venues d'outre-Atlantique, comme Election.com, deux autres projets, E-Poll et Cybervote, constituent la tête de file des initiatives européennes sur le sujet du vote électronique en ligne.

3.4.1 E-Poll.

Le projet européen E-Poll aboutira à une expérience de vote à des élections officielles par Internet dès 2002. Des urnes électroniques avec carte à puce et lecteur d'empreintes digitales seront déployées dans deux hôpitaux en France et huit en Italie. La généralisation du procédé est prévue en 2005 et permettra à toute personne ne pouvant, pour quelque raison que ce soit, se rendre dans un bureau de vote de participer à un scrutin.
France Télécom R&D, le centre de recherche et développement de l'opérateur français, s'implique dans la conception de ce système de vote électronique qui facilitera la participation, à distance, à des élections de grande envergure. Il permettra pour la première fois à des électeurs européens de répondre massivement aux consultations démocratiques sans avoir à se rendre dans les bureaux de vote habituels. D'ici 2005, près de 350 millions d'électeurs pourraient ainsi disposer d'un système de vote électronique opérationnel, fiable et entièrement sécurisé. ***[France Télécom]***

Le vote électronique garantira par sa sécurisation, en toute légalité, l'authentification du votant et la confidentialité de son choix. Il répondra plus précisément aux contraintes des personnes en déplacement ou éprouvant des difficultés mobiles au moment des élections : salariés en mission ou d'astreinte sur leur lieu de travail, vacanciers, personnes âgées ou hospitalisées, malades...
Parmi les applications qui en découlent figure la création de galeries virtuelles de présentation des candidats et de programmes électoraux multimédias. Le recours au vote électronique devrait également contribuer à réduire le volume des impressions papier nécessaire pour ce type d'élection (environ 3.500 tonnes pour une campagne européenne).

L'appareil que France Télécom R & D met au point devrait être une sorte de deux en un, à la fois urne et isoloir. Un drôle d'engin mi-technologie, mi-tradition car les votants seront identifiés par leurs empreintes digitales (technique de biométrie) et choisiront leur candidat sur un écran tactile, mais l'engin sera surmonté d'une tringle à rideau réglementaire comme pour un isoloir classique.
Le système comportera donc des urnes électroniques, un serveur dédié chargé du comptage et un réseau sécurisé pour la transmission. L'urne électronique, après insertion d'une carte à puces équipée d'un lecteur d'empreintes digitales, permettra à chacun de s'authentifier puis de s'informer sur les programmes de campagne et suivre sur un écran tactile les consignes liées au déroulement du vote. Transmis à un serveur dédié, le vote de l'électeur sera comptabilisé et dépouillé en toute sécurité par traitement informatique. L'ensemble des votes sera alors intégré aux résultats officiels de la consultation.

L'architecture du système sera transposable par la suite dans toutes les villes intéressées et adaptables à toutes contraintes de réseau, fixe à haut débit (ADSL) ou mobile à moyen débit (UMTS). L'ergonomie de l'urne et la conception globale tiendront compte des différentes législations en vigueur en Europe et de l'avis des pouvoirs publics.

Avant généralisation, une expérimentation validera les principes retenus. Des urnes mobiles expérimentales seront déployées au sein d'hospices et d'hôpitaux sur deux sites en France (Mérignac et Arcachon) et huit en Italie. En 2002, près de 8.000 personnes auront ainsi la possibilité de participer à des élections officielles par voie électronique. Cette expérimentation à grande échelle servira également à tester les usages inhérents au vote électronique, sa simplicité et sa convivialité d'utilisation.

Le projet E-Poll associe France Télécom, Siemens Informatique (le pilote du projet), la société informatique Sopra & Municipium, la région Aquitaine, le ministère italien de l'Intérieur, Ancitel (filiale informatique de l'Association des maires italiens) et l'organisme qui développe Internet dans les collectivités polonaises.

3.4.2 CyberVote.

Le *CyberVote* est le dernier programme retenu dans le cadre du quatrième appel d'offres IST (Information Society Technology), *Cybervote*, lancé le 1er septembre 2000. ***[Cybervote]***
Les promoteurs du projet entendent démontrer " la validité d'un système de vote en ligne à partir de terminaux Internet fixes et mobiles ".
Cybervote devrait proposer un service sur plusieurs plates-formes (PDA, téléphone mobile, et PC) agrémenté de solutions technologiques adaptées notamment pour ce qui est de garantir l'anonymat du suffrage exprimé.
Des tests grandeur nature seront effectués début 2003 dans trois pays de l'Union, en France (Issy-les-Moulineaux), en Allemagne (Brême) et en Suède (Kista).

CyberVote, "un système innovant de vote en ligne à partir de terminaux Internet fixes ou mobiles", est un projet de recherche et développement (RDT) co-financé par la Commission européenne et les industriels et organisations participants.
Le projet a officiellement démarré le 1 septembre 2000 et il se terminera le 1 mars 2003.
Le budget global s'élève à 3.243.629 Euros et représente un effort total de 27,4 homme par an.

La réalisation du projet *CyberVote* fait appel à des partenaires européens organisés en un consortium piloté par Matra Systèmes & Information.
Ce consortium regroupe :

Des partenaires industriels :
- Matra Systèmes & Information en France.
- Le centre de recherche de Nokia en Finlande.
- Le centre de recherche de British Telecom au Royaume Uni.

Des partenaires universitaires :
- L'Université de Leuven en Belgique.
- L'Université de Eindhoven aux Pays-Bas.

Des partenaires utilisateurs :
- La ville de Brême en Allemagne.
- La Ville d'Issy-les-Moulineaux en France.
- L'arrondissement de Kista/Stockholm en Suède.

L'objectif du projet *CyberVote* est de réaliser et de démontrer un système de vote en ligne intégrant un protocole de vote par Internet hautement sécurisé et vérifiable, et conçu pour être utilisé dans des élections de niveau local, régional, national et européen.
Il reposera sur un protocole de vote innovant spécialement créé pour le projet basé sur l'utilisation d'outils avancés de cryptographie. Comme cet objectif ne peut pas être atteint par une simple combinaison d'outils de cryptographie, des protocoles cryptographiques particuliers seront utilisés pour implémenter l'ensemble des propriétés de sécurité requises. Ce protocole assurera l'authentification des électeurs, l'intégrité et la confidentialité de leur vote lors de son envoi par Internet mais également lors du dépouillement et de la phase de vérification des votes. Il permettra aux électeurs de voter en totale confidentialité en garantissant leur anonymat dans toutes les phases du vote.

Le projet analysera également les législations en vigueur au sein des pays participants afin de déterminer d'une part, les exigences que le système doit satisfaire et d'autre part, de réfléchir aux éventuels amendements à proposer pour son utilisation dans un cadre légal en Europe.

.

4 Grille d'analyse comparative des implémentations sur base des règles.

4.1 Exemples de systèmes Vs Types d'implémentations.

A l'aide du tableau suivant, nous pouvons définir le type d'implémentation d'élection *I-Vote* ou *E-Vote* pour chaque système présenté précédemment (cf. chapitre 1.6 Types d'implémentations).

Pour rappel, cette définition se base sur la position en "Local" ou à "Distance" des trois éléments principaux d'un système d'élection électronique, c'est-à-dire :

- L'authentification de l'électeur.
- La station de vote.
- L'urne électronique.

Implémentation Vs Systèmes	**Vote automatisé en Belgique**	**Le système S.V.I. de Nedap**	**Primaires Arizona I-Vote dans bureau**	**Primaires Arizona I-Vote sur Pc privé**
Authentification de l'électeur	Local	Local	Local	Distance
Station de vote	Local	Local	Local	Distance
Urne électronique	Local	Local	Distance	Distance
Implémentation	E-Vote	E-Vote	I-Vote	I-Vote
Type d'élection	Vote électronique dans un bureau traditionnel sans connexion au réseau.	Vote électronique dans un bureau traditionnel sans connexion au réseau.	Vote électronique via des terminaux ou ordinateurs de vote.	Vote électronique sur ordinateur à distance offert à tous les électeurs.

4.2 Règles et Contraintes Vs Exemples de systèmes.

Comparons les différents systèmes d'élections présentés sur base des 20 règles définies précédemment (chapitre 1.5 Traduction en règles et contraintes).

Règles Vs Systèmes	***Vote automatisé en Belgique***	***Le système S.V.I. de Nedap***	***Primaires Arizona I-Vote dans bureau***	***Primaires Arizona I-Vote sur Pc privé***
1 Anonymat de l'électeur	Oui Par identification en dehors du système.	Oui Par identification en dehors du système.	Oui Par séparation des données.	Oui Par séparation des données.
2 Secret du vote	Oui Par chiffrement	Oui Par chiffrement	Oui Par chiffrement	Non Risque de vision sur l'ordinateur personnel.
3 Intégrité	Oui Isoloir	Oui Isoloir	Oui Isoloir	Non Risque d'influence.
4 Procédure de vérification pour l'électeur	Oui	Non	Non (uniquement confirmation réception)	Non (uniquement confirmation réception)
5 Outils et procédures d'audit	Oui Recomptage des cartes magnétiques et contrôle du président de bureau.	Non	Oui	Oui
6 Garantie du secret lors des audits	Oui	Oui	Oui	Oui
7 Election complète à 100%	Oui	Oui	Oui	Oui

Règles Vs Systèmes	***Vote automatisé en Belgique***	***Le système S.V.I. de Nedap***	***Primaires Arizona I-Vote dans bureau***	***Primaires Arizona I-Vote sur Pc privé***
8 Identifier un vote incorrect	Oui	Oui	Oui	Oui
9 Autoriser vote blanc	Oui	Oui	Oui	Oui
10 Modèles multiples de bulletins de vote	Oui	Non	Oui	Oui
11 Redondance des canaux d'informations	Oui Cartes + Compteurs électroniques	Non	Oui	Oui
12 Structure de contrôle et de sécurité	Oui	Oui	Oui	Oui
13 Indépendance technologique	Oui	Oui	Oui	Oui
14 Présentation adaptée à l'électeur	Oui	Non	Oui	Oui
15 Ouverture sur l'extérieur	Oui	Non	Oui	Oui

Règles Vs Systèmes	***Vote automatisé en Belgique***	***Le système S.V.I. de Nedap***	***Primaires Arizona I-Vote dans bureau***	***Primaires Arizona I-Vote sur Pc privé***
16 Opération de vote rapide	Oui	Oui	Oui	Oui
17 Mobilité	Oui	Oui	Oui	Oui
18 Efficacité	Oui	Oui	Oui	Oui
19 Variabilité de la durée	Oui	Oui	Oui	Oui
20 Modification du vote par l'électeur	Non, cette règle n'est pas d'application pour les élections officielles.			

4.3 Résumé des problèmes par systèmes.

En conclusion du tableau d'analyse des règles et contraintes, nous pouvons identifier les problèmes pour les systèmes présentés.

Règles Vs Systèmes	***Vote automatisé en Belgique***	***Le système S.V.I. de Nedap***	***Primaires Arizona I-Vote dans bureau***	***Primaires Arizona I-Vote sur Pc privé***
Numéros des règles ou contraintes posant problèmes	-	4,10,11,14,15	4	2,3,4
Commentaires	Le système de vote automatisé belge respecte globalement l'ensemble des règles. Néanmoins, la procédure de test appelée "*vote de référence*" et effectuée par le président de bureau est trop limitée et non complète pour réellement prouver l'intégrité du système.	Le système Nedap présente de nombreux problèmes dans le respect des règles : • Pas de vérification par l'électeur • Modèle de bulletin fixe • Manque de redondances de l'info • Présentation non adaptable à l'électeur • Système non ouvert sur l'extérieur	Le système de Election.com utilisé dans les primaires en Arizona pour les votes à partir de stations à voter, dans des bureaux de votes, respecte les règles à l'exception de la mise en place d'une réelle procédure de contrôle par l'électeur de son vote. Néanmoins l'électeur reçoit une confirmation d'arrivée et d'acceptation de son vote par le système informatique des élections.	Le système de Election.com utilisé dans les primaires en Arizona pour les votes à partir d'ordinateurs personnels présente quelques problèmes dans le respect des règles : • Manque de vérification par l'électeur en dehors du message de confirmation. • Risque pour le secret du vote lorsqu'il n'y a pas d'isoloir. • Risque pour l'intégrité car influence et collusion possible pour les votes à domicile.

Conclusion

Suite à la première élection officielle sur Internet, organisée par le parti démocrate d'Arizona pour les primaires aux présidentielles en mars 2000, le vote électronique a acquis une dimension et une crédibilité nouvelle, qui engendre quelques interrogations.

Les règles principales de secret, d'intégrité et de confidentialité étant remplies, et les techniques de sécurisation des réseaux étant de plus en plus performantes, on peut alors raisonnablement penser que ce système va se répandre dans nos démocraties, mais avec quelles conséquences ?

A Bruxelles, la Commission apporte son soutien et subventionne plusieurs projets d'origine européenne (*E-Poll* et *CyberVote*) et un pays comme l'Allemagne annonce des élections officielles à distance dès 2006 et pour l'Italie ou les Pays-Bas à partir de 2003.

Les expérimentations se focalisent beaucoup sur l'élection de la représentation nationale et locale. De ce point de vue, le vote électronique a un effet positif puisqu'il contribue à faire chuter le taux des abstentions de façon très significative. Les primaires démocrates ont connu une progression de plus de 600% de participation. En outre les économies et la simplification des procédures sont également très importantes.

Mais quelques uns objecteront, dans nos vieilles démocraties, que le vote est un geste dont la charge symbolique "nécessite un minimum d'efforts".
Réduire cet acte essentiel à l'envoi d'un simple signal virtuel est certes perturbant mais tout de même pas inconcevable.
Tous les électeurs pratiquant le vote par correspondance seront satisfaits de trouver une solution de substitution sur Internet. Quant aux autres, ils auront le choix entre le bureau de vote électronique et le vote à domicile avec accès sécurisé.
En Belgique, il semble probable que l'avantage du vote électronique "à distance" restera limité en raison des taux de participation élevés que connaît notre pays car le vote y est obligatoire, de la proximité des bureaux de vote et de l'interdiction du vote par correspondance.

Le vote électronique pourrait aussi favoriser le développement de la consultation directe des citoyens, notamment dans le cadre des référendums d'initiative populaire au niveau local. L'effet de ces référendums ne sera pas sans conséquences sur le mode de gestion des institutions.
Jusqu'à présent, dans un système de consultation traditionnel, de tels référendums étaient rares, généralement organisés dans le cadre de décisions sensibles à prendre au niveau d'un territoire : augmentation des impôts, installation de la télésurveillance, d'une usine d'incinération, choix entre le métro ou le bus dans une ville...
Un Internet généralisé et sécurisé simplifiera l'organisation de telles consultations et favorisera leur multiplication. Les risques d'abus de nature à bloquer les capacités de gestion des élus sont à redouter. Même si cela fait un peu peur, on doit s'attendre, via Internet, à une plus grande réactivité de la part des citoyens et peut-être aussi à l'apparition de "référendums sauvages" pour exercer un maximum de pressions sur certaines décisions.

Une enquête de "*Opinion-Way*" indique que 80 % des citoyens internautes seraient prêts à envoyer un message de protestation par e-mail à une personnalité publique et 85% à signer une pétition. ***[Opinion Way]*** Dans un tel contexte il sera nécessaire d'imaginer de nouvelles formes de "gouvernance" intégrant ces procédés de consultations directes. Elles devront être crédibles (pour désamorcer les initiatives sauvages) sans obliger les élus à s'en remettre au suffrage populaire pour n'importe quelle décision, ce qui serait la négation de notre système démocratique.

La grille d'analyse des règles et contraintes d'un système de vote nous a montré que les organisations de vote en ligne les adoptent déjà presque toutes, et même plus que pour d'autres systèmes non connectés à un réseau. Il ne reste plus que des problèmes d'éthiques liés à l'absence de déplacement d'un électeur dans un bureau de vote.

A l'heure actuelle, seul un faible pourcentage de la population est connecté à Internet. En outre, les inégalités entre le Nord et le Sud de la planète dans ce domaine sont flagrantes. Le "peuple virtuel", dans notre pays comme dans de nombreux autres pays, est jeune, souvent masculin et relativement bien qualifié. Ce qui pose question dans la représentativité de ce citoyen virtuel. ***[Lobet]***

Cependant, avec le développement rapide et croissant d'Internet, le vote en ligne et ses dérivés sont promis à un brillant avenir. Et il y a fort à parier que les barrières politiques, juridiques et culturelles s'effaceront rapidement, tant l'avènement de la démocratie électronique semble incontournable, pour garantir la pérennité des systèmes politiques actuels.

Bibliographie & Références

[A.P.P.D.D]
www.appdd.org, Association pour la promotion de la démocratie directe.

[Adler 2000a]
CryptoCrypto 101 Technical Brief 2000 by Jim Adler President & CEO VoteHere.net

[Adler 2000b]
Online Voting Sécurity 2000 by Jim Adler President & CEO VoteHere.net

[Bio & Secu]
Revue Corporate.net du 21 juin 2001, Biométrie et Sécurité "Bientôt, la fin du numéro d'identification personnel".

[Cita]
www.fundp.ac.be/recherche/projets/fr/01298502.html, Cellule Interfacultaire de Technology Assessment, Projet EUSV 2001-2002

[Cranor's]
www.research.att.com/~lorrie/voting/hotlist.html, List of links to Internet Sites with electronic-voting related information.

[Cybervote]
www.eucybervote.org, "An Innovative Cyber Voting System for Internet Terminals and Mobile Phones".

[Dictson & Ray 1]
Internet Voting: Essential Knowledge for Policymakers by Derek Dictson & Dan Ray

[Dictson & Ray 2]
White paper "The modern democratic revolution: an objective survey of Internet based elections"

[Driss Chraïbi]
Romancier marocain, citation extraite de "La foule" Publication : DENOEL 01/06/1982
ISBN : 220720314X

[Election.com]
www.election.com, "The Global Election Company" Informations techniques et Elections Primaires Démocrates.

[Elliot]
Examining Internet Voting in Washington by David Elliott, Assistant Director of Elections

[EuStudent]
L'EUSV site www.eu.studentvote.org

[Felten & Balfanz]
"Web Spoofing An Internet Con Game", Edward W. Felten, Dirk Balfanz, Drew Dean and Dan Wallachn Technical Report 540-96, Department of Comuter Science, Princeton University.

[Forum démocratie]
www.issy.com/e-democratie, Deuxième forum de la démocratie à Issy-Les-Moulineaux (France) 17 mai 2001

[France Télécom]
www.francetelecom.fr, "France Telecom préparent le vote électronique de demain"

[Guill.net]
Guill.net - La page des réseaux, www.guill.net (sécurité, RPV & VPN, Authentification, Attaque, SSL, WTLS, IP Spoofing, Cryptographie).

[InternetAddict]
www.internetaddict.be, "La Belgique testera bientôt la carte d'identité digitale" 7/8/2000

[Jones]
California Internet Voting Task Force "A Report on the Feasibility of Internet Voting" by Bill Jones Secretary of State

[Lobet]
Démocratie électronique et citoyenneté virtuelle, Claire Lobet-Maris & Béatrice van Bastelaer, Wallonie, 62, mars 2000, pp.57-67

[M.I. dpt elec]
Ministère de l'Intérieur, Direction des Elections et de la Population, notes techniques sur les systèmes Digivote et Jites, Elections Provinciales et Communales du 8 octobre 2000.

[M.I. Elec. 2000]
Ministère de l'Intérieur "Les élections communales et provinciales 2000", guide de présentation.

[M.I. Pres. Bur]
Ministère de l'Intérieur Directive administratives destinées aux présidents des bureaux de vote automatisé - version 3 - 9/8/2000.

[M.I. Vote Electronique]
Ministère de l'Intérieur, Direction des Elections et de la Population, www.elections.fgov.be

[Moniteur Belge]
Moniteur Belge, journal officiel, publication de la loi organisant le vote automatisé, 11 avril 1994.

[Nedap]
Nedap/France Election "le système S.V.I."

[Opinion Way]
www.opinion-way.fr,"*Les Internautes et l' e-démocratie*" Enquête réalisée par Opinion-Way du 4 au 6 septembre 2000 par interview effectué en ligne auprès d'un échantillon de 455 personnes représentatif de la population des internautes français.

[Pour EVA]
www.poureva.org, Association pour une Ethique du Vote Automatisé

[Safevote]
www.sofevote.com, Informations techniques et tests d'attaques.

[Salford City]
Electroninc voting and counting scheme, Evalutation Report, August 2000

[SecurePoll]
www.SecurePoll.com, Collection of Internet voting information on the net.

[The Bell]
The Bell Newsletter, Privacy, Security and Technology In Internet Voting, www.thebell.net, (Decembre 2000 & February 2001 "Voting System Requirements").

[Turner-Drozdova]
Powerpoint présentation "An overview of On-Line Voting : systems and issues", Jon Turner, Ekaterina Drozdova, Anil Nileshwar, prepared for : Conférence on democracy, integration and the internet, New York march 2001

[VoteHere]
www.votehere.net, "The secure internet voting company"