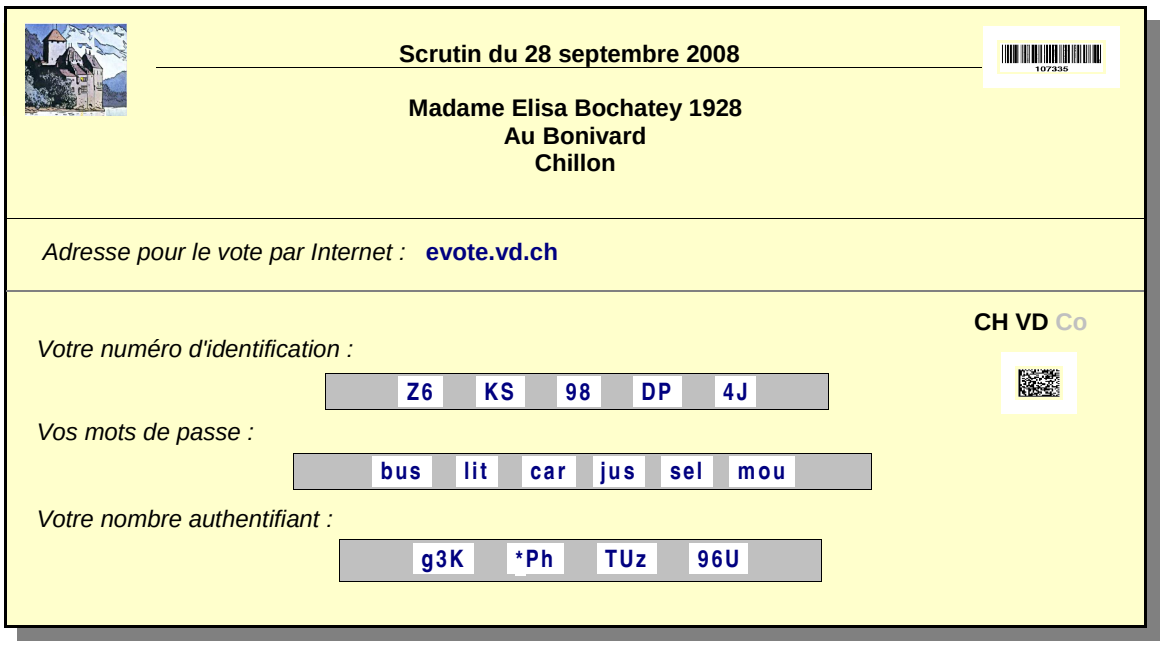
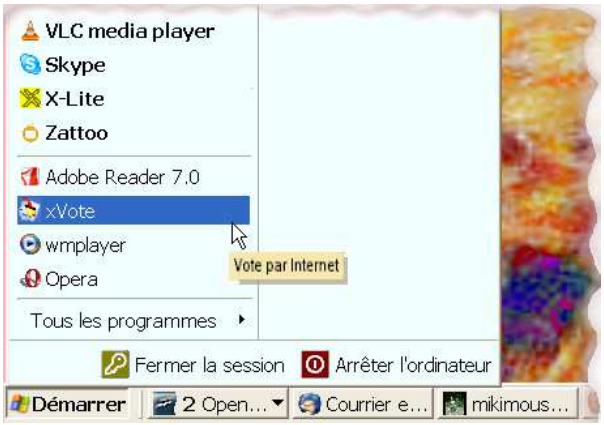
## Lancement

Le citoyen reçoit sa carte de vote par la poste[1], comme actuellement pour le vote par correspondance ou au local. La seule différence est que cette carte est complétée par l'adresse de vote (*URL*), et trois champs individuels contenant des codes d'identification et d'authentification[2].




Au lancement, l'application effectue une vérification de la qualité de ses modules exécutables ou d'interface utilisateur.
C'est-à-dire qu'elle vérifie leur authenticité (ils proviennent bien de nos développeurs) et leur intégrité (ils n'ont pas été corrompus par la suite).



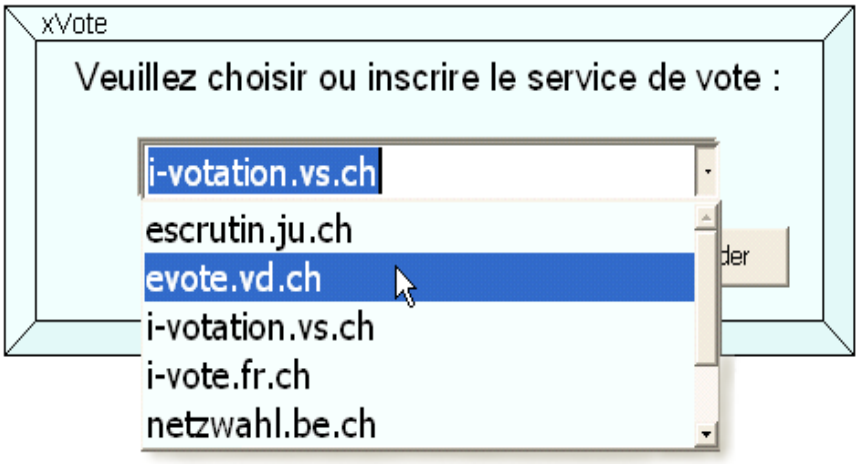

Elle vérifie ensuite si elle doit ou devrait être mise à jour. Selon le cas, elle effectue cette mise à jour de manière sécurisée et automatique.

Enfin, elle obtient et maintient divers éléments pour la sécurisation des transactions, particulièrement l'état actuel des clefs de sécurité des divers serveurs qui seront impliqués durant l'opération.

1 Un citoyen ayant reçu son identité numérique, et tant que celle-ci est valide, peut opter pour recevoir sa carte de vote par courriel sécurisé (signé et chiffré).
2 La carte et son contenu sont montrés en couleur à titre d'illustration, en réalité l'impression est en noir sur blanc. La carte pourrait aussi rappeler l'empreinte pour vérifier le certificat du site de chargement *initial* du logiciel.

## Phase 0 initialisation

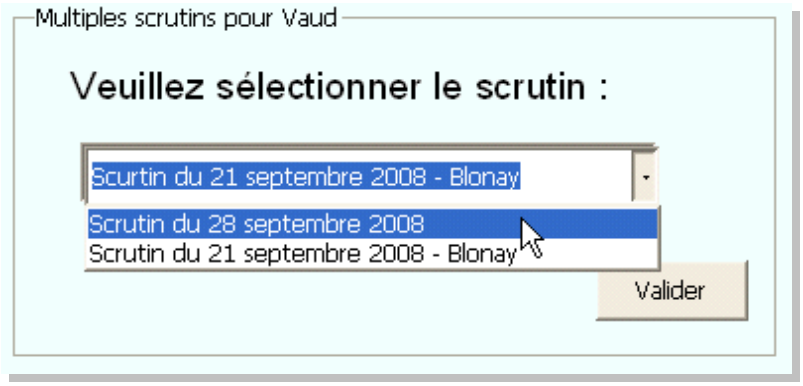
L'application demande de vérifier, de changer ou d'inscrire le nom du serveur de vote par internet. Dans le cas d'un vote ou d'une élection officielle, il s'agit du serveur relié à l'administration publique dont relève le citoyen; par exemple, en Suisse, de son canton.




---

À partir de ce choix, l'interface utilisateur riche est activée selon le domaine choisi, et les dialogues suivants ne sont que des exemples simplifiés d'une interaction qui peut-être adaptée, illustrée, animée, réactive, informative, etc.

---



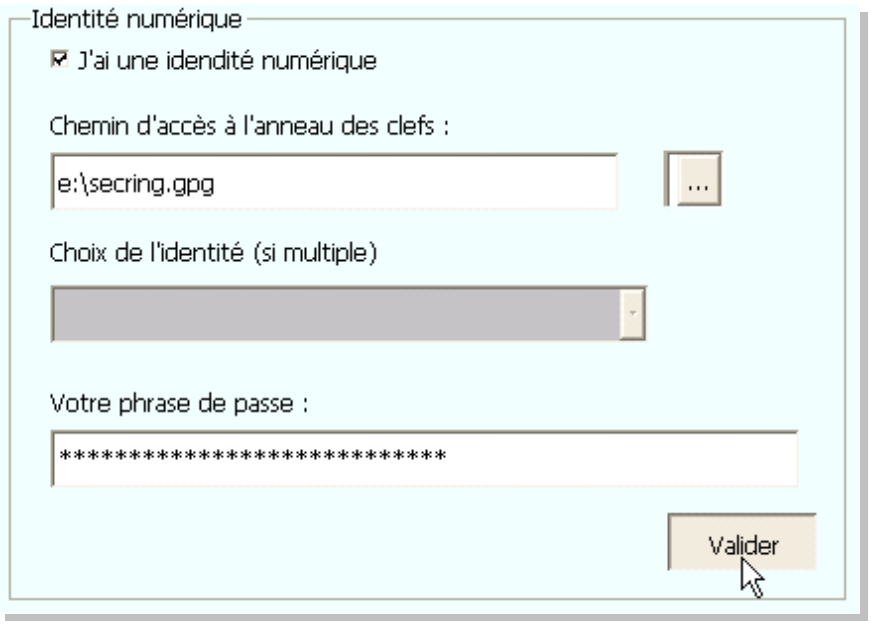

S'il y a *plusieurs scrutins en cours simultanément pour le domaine de vote choisi*, l'application demande pour lequel l'opération doit avoir lieu (s'il n'y a qu'un seul scrutin en cours dans le domaine, ce dialogue est bien sûr évité).

## Phase 1 identification

### *Cas où le citoyen a déjà une identité numérique*

L'application demande alors si le citoyen possède déjà une identité numérique, ce qui est le cas s'il a déjà voté par internet. Et dans ce cas, l'application l'invite à confirmer ou indiquer où elle se trouve (de préférence sur une clef USB à brancher), si -et seulement si- plusieurs identités se trouvent dans l'anneau présenté, l'application demande de confirmer ou sélectionner celle à utiliser.

Enfin, la phrase de passe permettant de déverouiller (la clef privée de) l'identité est requise.




Si l'identité fournie est forte ou fraîche, **l'application passe ensuite directement à la phase 3 pour l'habilitation**.

→ voir page 5

Si l'identité doit être renouvelée, **l'application passe alors à la phase 2 simplifiée.**

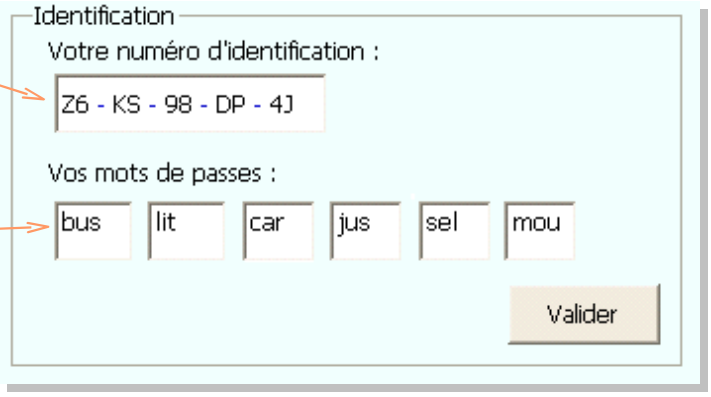
→ voir page 4

### *Cas où le citoyen n'a pas encore d'identité numérique*

Si le citoyen n'a pas encore d'identité numérique (ou l'a perdue), ou si son identité n'est plus valable[3], l'application demande le numéro d'identification et les mots de passe figurant sur la carte de vote reçue.

Le numéro d'identification est formé d'une suite de cinq paires de chiffres ou de lettres majuscules, il permet plus de *mille milliards* de combinaisons.

Les mots de passe sont six petits mots simples de trois lettres chacun, ils offrent aussi plus de *mille milliards* de combinaisons possibles.



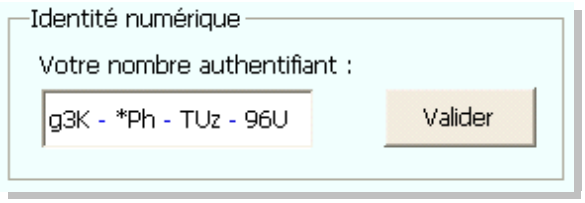

Notons que les deux derniers caractères du numéro d'identification sont des codes contrôle qui permettent d'immédiatement détecter une erreur de recopie ou de frappe de la part du citoyen. De même, le dernier élément des mots de passe est aussi un code détecteur d'erreurs.

3 Si l'identité numérique n'est plus valable à la date du scrutin, le citoyen reçoit automatiquement une carte par voie postale. Si l'identité est encore valable à la date d'envoi des liasses de votes, il reçoit aussi le courriel sécurisé.

## Phase 2 cyberidentité

### *Renouvellement de la cyberidentité (cas de la phase 2 simplifiée)*

Si l'identité numérique existe déjà, mais qu'elle doit être renouvelée, l'application demande uniquement au citoyen son nombre authentifiant, qui figure sur sa carte de vote, reçue par poste, ou sur le courriel sécurisé alternatif.




Ici aussi, les deux derniers caractères forment un code détecteur d'erreur.

Le nombre authentifiant est formé de quatre groupes de trois caractères chacun comprenant des lettres majuscules ou minuscules (la casse est significative), des chiffres ou certains caractères spéciaux figurant sur le clavier. Le nombre authentifiant permet plus d'un milliard de milliards de combinaisons. Il n'est pas transmis, mais sert à relever un défi cryptographique équilibré entre le serveur et l'application.

L'application passe ensuite en phase 3 ou "habilitation" pour l'obtention du droit de vote

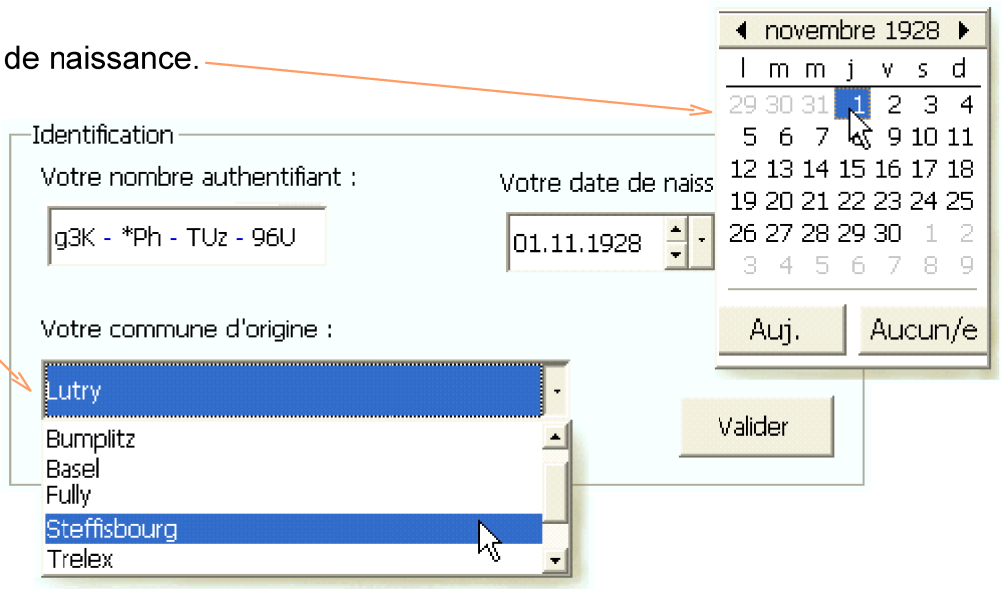
→ voir page 5

### *Création de la cyberidentité (cas de la phase 2 complète)*

Si le citoyen n'a pas encore (ou plus) d'identité numérique, l'application va lui demander le nombre authentifiant et deux informations personnelles pour l'authentifier :

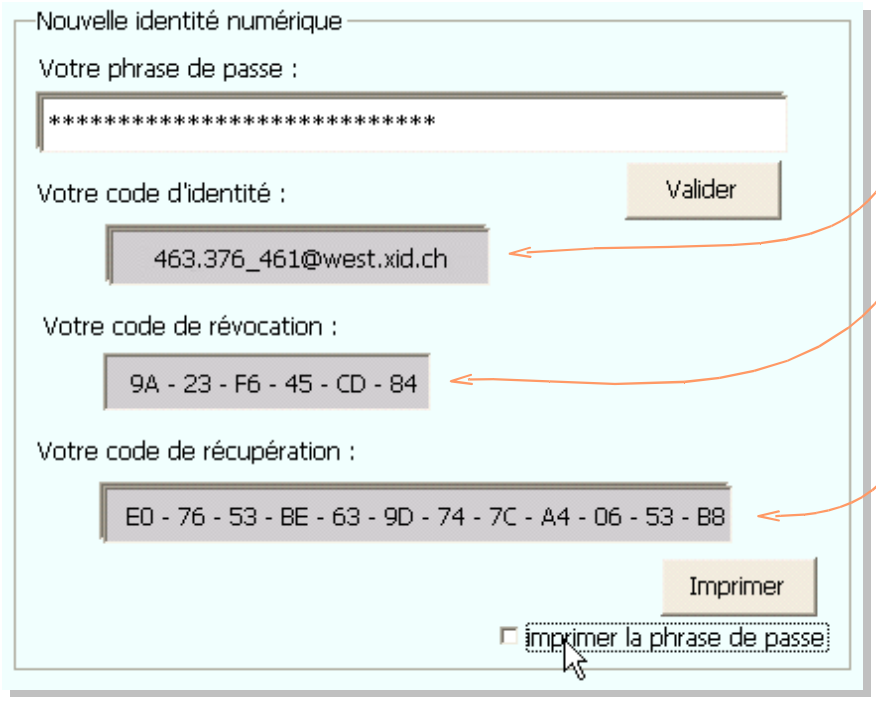
L'une est sa date de naissance.

L'autre est sa commune d'origine[3] (dans une liste de communes classées alpha-bétiquement).




4 Ou équivalent pour l'électeur étranger (lieu de naissance).

Le citoyen, ayant été correctement authentifié, reçoit alors son identité numérique[5] qu'il verrouille en donnant une phrase de passe.



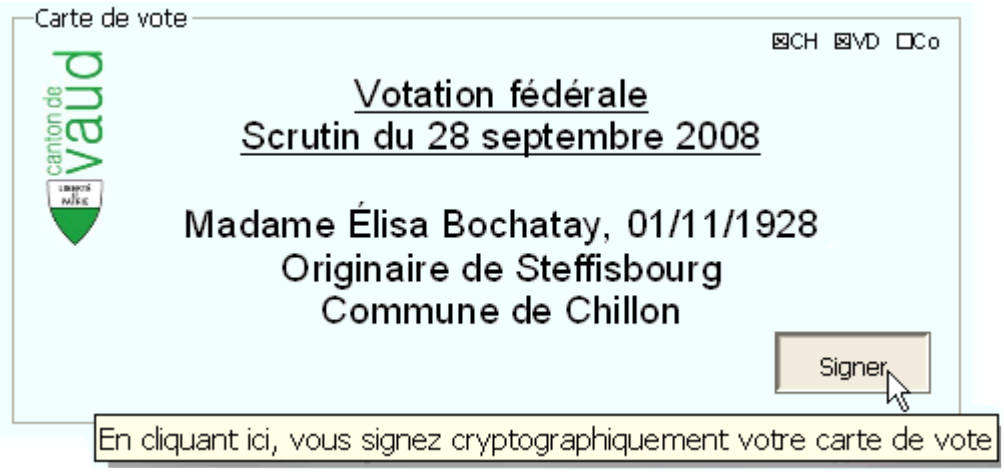

Trois codes sont affichés :

- le code identifiant le porteur pour le service d'identité numérique (à titre purement interne);
- un code permettant de révoquer (annuler) l'identité numérique en cas de perte ou atteinte à celle-ci;
- enfin, un code permettant de récupérer la clef chiffrante, en cas de perte de l'identité numérique (p.ex. oubli de la phrase de passe), et ainsi déchiffrer les documents chiffrés (p.ex. les courriels sécurisés reçus).

Il lui est conseillé d'imprimer ou noter ces codes, et de les conserver dans un endroit sûr.
*Ils ne seraient utilisés qu'exceptionnellement, en cas de perte de l'identité numérique.*

## Phase 3 habilitation (obtention du droit de vote)

Venant directement de la phase 1 d'identification ou à la suite de la phase 2 de cyberidentité, le citoyen doit signer sa carte de vote[6] dématérialisée.




5 Cette identité est standard, et pourra aussi être utilisée par le citoyen pour sécuriser d'autres usages d'Internet

6 Il est évident que, si le citoyen a déjà voté par internet, ou que son vote a déjà été enregistré par correspondance ou au local de vote, les serveurs refuseront de lui délivrer un droit de vote. De même, immédiatement après un vote parfait par internet, l'enregistrement du vote par correspondance ou la présentation au local de vote sera bloqué.

Ce faisant, il reçoit en contre-partie un droit de vote unique et anonyme pour le scrutin en question, et lié à sa commune de résidence officielle.

Comme à chaque étape, le citoyen peut s'interrompre[7], et même changer d'ordinateur, avant de passer à l'étape suivante au moment où il le désirera. En relançant l'application, il lui sera seulement demandé de présenter son identité numérique, puis l'application se placera automatiquement à l'étape suivante du vote en cours.

## Phase 4 vote

Le bulletin de vote est présenté au citoyen, sous la forme d'un formulaire Web, avec les contrôles adaptés aux diverses questions : choix oui/non, intiative/contre-projet, candidats à un/des poste(s), etc...

L'application permet le vote et l'élection, et ce, quelle qu'en soit la complexité.


Après avoir pressé **Valider**, et ainsi scellé son contenu, le citoyen est requis de vérifier les choix effectués

En donnant l'ordre **Envoyer**, citoyen provoque chiffrement du bulletin par la clef de l'Urne de son domaine de vote et son dépôt sécurisé au local de vote virtuel.


le
le

7 Il peut aussi suspendre les opérations sans quitter l'application, mais -passé un certain délai- il devra recommencer l'identification pour raison de sécurité.

## Phase 5 contrôle

Pour garantir encore plus l'anonymat de son vote, le bulletin n'est pas déposé immédiatement dans l'urne virtuelle finale, mais transite (anonymement aussi) par le serveur de scrutation faisant office de local de vote virtuel[8].

En effectuant le contrôle, ou le ré-effectuant ultérieurement à volonté, le citoyen verra donc d'abord s'afficher un reçu du serveur de scrutation, puis -après un laps de temps aléatoire- c'est le récépissé de l'urne qu'il recevra. Ce récépissé est anonyme, mais lié indirectement par l'estampille (anonyme) à la qualité personnelle d'électeur du citoyen. Il relève donc du bulletin unique et personnel du citoyen.


La teneur du bulletin est masqué par le chiffrement avec la clef (publique) de l'Urne effectué sur le poste du citoyen, ceci *sans la moindre possibilité de dévoilement jusqu'à l'issue du scrutin* et la recombinaison des parties de la clef privée par la commission électorale des scrutateurs. Cette recombinaison permettant le déchiffrement du contenu de l'Urne.

À l'issue de la votation, lors de l'ouverture et dépouillement de l'urne, ce sont des bulletins entiers qui seront ouverts (déchiffrés) avec les questions telles que présentées au citoyen et ses réponses telles qu'il les a vérifiées.

Les bulletins dématérialisés sont estampillés anonymement par le citoyen, selon le scrutin et la circonscription du citoyen, et validés selon ses droits de vote. *L'estampille virtuelle est unique et figure cryptographiquement la qualité d'électeur personnelle et anonyme du citoyen et scelle le contenu du bulletin.* Elle garantit aussi que ce contenu du bulletin, les choix ou motivations du citoyen, n'a pas été modifié après le scellement et la vérification de celui-ci par le citoyen.

---

Le résultat du scrutin par internet est donc totalement contrôlable et recomptable par toute commission tierce.

---

8 Le droit de vote anonyme reçu par le citoyen est unique, il n'est donc pas possible de voter deux fois. Le deuxième dépôt de bulletin (même différent de contenu) serait refusé tant par le serveur de Scrutation que par l'Urne.

**Démocratique** – respect des règles et de l'esprit

Universalité : Tous les citoyens accèdent également au vote : expatriés, infirmes, voyageurs, vieillards, malades

Unicité : Chaque électeur a une et une seule voix !

Temporalité : Les suffrages ne sont dépouillables qu'après la clôture.

Généralité : Le vote électronique favorise la participation, en particulier il évite l'abstentionisme des jeunes.

**Exact** – chaque voix est comptabilisée

Authenticité : Un vote n'est valide que s'il provient d'un citoyen légitime.

Intégrité : Un vote n'est valide que s'il contient la motivation originelle du citoyen,

Exhaustivité : Un vote valide ne peut être supprimé.

Complétude : Un faux vote ne peut être ajouté.

**Privé** – anonymat et secret inconditionnels

Secret : Il n'est pas possible de connaître le contenu d'un vote.

Anonymat : Il n'est pas possible de relier un bulletin avec un votant.

Incessibilité : Pas de vote par procuration ou de vente de vote -l'acte est strictement personnalisé et un électeur ne peut pas prouver ce qu'il a voté.

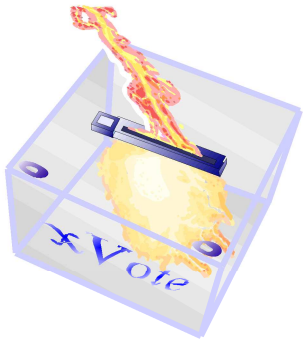
**Auditable** – contrôlable en tous temps et par tous

Audit antérieur : L'ensemble du système est auditable statiquement préalablement.

Audit dynamique : La commission électorale -indépendante- surveille les opérations, grâce à une unité informatique séparée, et peut s'assurer que le processus est juste.

Audit interne : L'ensemble des processus informatiques est analysable par l'activité des réseaux locaux (boîte blanche).

Audit postérieur : Chaque opération élémentaire est prouvable (statiquement ultérieurement).




**Confortable** – simple et souple

Tout électeur a la possibilité de voter :

- rapidement et efficacement,
- avec un équipement courant,
- par une installation automatique,
- sans capacité ou connaissance particulière,
- dans le lieu où il se trouve,
- au moment où il le désire.

**Flexible** – pour tout et pour tous

Différents niveaux

- Global (fédéral),
- Régional (cantonal),
- Local (communal),

Les votations pures

- choix Oui/Non,
- multi-choix exclusif ou inclusif flexibles.

Les élections

- choix par listes et noms sous divers critères.

Pleinement adaptable par des règles dynamiques

Un nombre quelconque d'électeurs

Partitionable (multi-administration)

Multilingue

**Mobile** – partout et en tout temps

Le système permet de voter :

Depuis n'importe où (globalité).

Par n'importe quel réseau (interopérabilité).

Sur tous systèmes (portabilité)

- MS-Windows (dès Win98),
- Mac OS X (Apple),
- Linux, etc.

Avec tous types d'équipement (multi-plateforme)

- Ordinateur personnel (PC), Organiseurs, Ultra-Mobile PC, Mobile Internet Devices, Smartphones...

**Sûr** – en toute sécurité et en toute fiabilité

Le système garantit :

- La confidentialité, l'authenticité et l'intégrité des transmissions,
- La sécurité des serveurs et la disponibilité des données,
- La solidité contre les pannes et pertes de connexion.

Les processus de vote sont isolés du poste du votant au sein d'une machine virtuelle.

Les logiciels constituant le système assurent la fiabilité et l'efficacité et sont développés avec les outils des systèmes critiques (transport, finance, aéronautique, spatial, militaire).

Ces logiciels implantent l'ensemble des normes en vigueur.