Relations entre l'administration cantonale et xVote

En amont de la votation, l'Administration cantonale doit constituer un registre informatisé des électeurs, avec les extractions provenant des communes, et comprenant deux ou trois informations supplémentaires.

Durant le vote, l'Administration est informée en continu de la situation et peut opérer des mutations et des contrôles (dont la résolution de réclamations).

En aval, l'Adminisration supervise la bonne fin du vote, et réceptionne les résultats en les fusionnant avec ceux des communes.

Généralités

En standard, l'Administration cantonale ou les administrations communales peuvent directement accéder aux pages de commandes Web sécurisées (https, avec authentification forte de l'utilisateur) intégrées dans le serveur xVote.

Le registre des électeurs informatisé est une base de données se trouvant au sein de l'informatique cantonale, il doit durer durant toute la session de votation, et jusqu'à la fin de la période de recours. Il est ensuite détruit.

xVote ne conserve aucune donnée nominale.

À part, en amont, la constitution et le maintien du registre des électeurs, l'impression des cartes de vote (papier) et, en aval, la fusion des résultats du vote par internet avec les autres résultats, ainsi que leur publication, le service d'xVote couvre la totalité de la préparation, de la gestion et de la finalisation du vote par internet.

Les considérations plus techniques se trouvent dans le document de titre "Relations entre l'informatique cantonale et xVote" et de nom 20060111_1525.

Information continue

Durant toute la session, la situation courante peut être consultée à volonté grâce à l'accès aux pages d'information, publiques ou restreintes, du serveur Web intégré dans le serveur xVote.

De plus, les administrations peuvent recevoir une Information continue, et être notifiées immédiatement des éventuelles alarmes. via la messagerie instantanée[1] (clavardage ou *t*chat), le courriel (eMail) ou les textos[2] (SMS).

Les administrations peuvent enregistrer leur adresse (jabber ou courriel) avec la sélection de profils d'information ou d'évènements déclencheurs désirés.

La constitution et l'utilisation du registre des électeurs

Le registre des électeurs (R.E.) est constitué de la consolidation des registres fournis par

1 Le système xVote utilise la norme ouverte et décentralisée Jabber . Via les passerelles que possède Jabber, vers les autres systèmes de messagerie instantanée, il possible de recevoir le flux d'information par un autre protocole (MSN, AOL, Yahoo, ICQ, etc.), mais alors la possibilité de sécurisation du contenu (authenticité, confidentialité, intégrité) est perdue.

2 En fait courriel vers un numéro de mobile, via une passerelle Mél-à-SMS.

les communes du canton. Il doit comporter certaines informations complémentaires aux actuelles.
Essentiellement, il s'agit de :

- la date de naissance;
- la ou les commune(s) d'origine(s) pour un citoyen suisse;

ou

- une information personnelle[3], remplaçant la commune d'origine, et à choisir dans une liste, pour les étrangers si ceux-ci votent;

ainsi que

- le numéro d'identification unique stable[4] NNAS (nouveau numéro d'assurance sociale, délivré à tout résident à partir de 2007 et définitif à partir de 2008).

Ce dernier élément permet de relier l'identité numérique, sous la forme des clefs personnelles ou de leur certificat, au travers de leurs renouvèlements, avec le citoyen porteur.

Une requête d'initialisation générale des fiches des électeurs doit alors être faite à xVote (renseignements des trois chiffres : numéro d'identification -Internet-, mots de passe, nombre authentifiant -NI, MP et NA-, génération de la liste de choix pour la question authentifiante, vérification de la possibilité d'envoi de la carte dématérialisée, etc.).

Avec les informations contenues et collectées, les cartes de vote sont générées :

- soit classiquement (pour impression papier), si xVote a indiqué qu'il n'est pas demandé ou pas possible d'envoyer par courriel;
  elles comportent, outre l'habituel numéro d'électeur NE (le N° de carte), les valeurs personnelles NI, MP et NA (numéro d'identification -Internet-, mots de passe, nombre authentifiant).
- soit -à bonne date- de manière dématérialisée et sécurisée par xVote, si une adresse courriel acceptée est présente (eMail) avec un certificat valide à la date du scrutin.

Dans ce dernier cas, c'est un courriel qui est envoyé par xVote à l'adresse électronique, contenant (entre autres) :

- la date du scrutin;
- le nom du citoyen;
- sa commune de domicile politique;
- son numéro d'électeur NE (le N° de carte)
- ses capacités de vote (fédéral, cantonal, communal);
- ainsi que les valeurs personnelles NI, MP, NA;
- l'adresse du vote (nom de [sous-]domaine du serveur).

Il contient aussi un lien vers une version Portable Document Format (PDF) permettant d'imprimer une carte de vote pour voter selon les moyens traditionnels.

3 Typiquement le lieu officiel de naissance.
4 L'identité numérique a un sous-jacent (clef/certificat) qui est labile de par les renouvèlements périodiques, il faut un élément d'intermédiation, entre l'identité numérique et le système de vote électronique, donnant une identification permanente, c'est ce numéro unique d'identification NNAS.

Le courriel est envoyé signé par la clef de l'administration de vote (avec son certificat annexé) et chiffré sous la clef garantie du citoyen.

Durant la session de votation

Il est toujours possible pour une commune d'opérer des mutations (ajout, suppression) dans le Registre des Électeurs, y compris de résoudre des réclamations (sp. obtention d'une nouvelle carte de vote).

L'ajout d'un électeur se fait sans autre, il faut juste effectuer finalement une requête à xVote (en donnant NE) pour qu'il renseigne les valeurs pour les codes du vote internet (NI, MP et NA); ceci avant d'imprimer la carte pour le (nouvel) électeur.

Les mutations (corrections) d'une fiche d'un électeur n'ont de sens que si celui-ci n'a pas encore voté ou commencé une opération de vote (état "pas_voté" = (0;-)).

La suppression (pour départ de la circonscription, ou décès) peut se faire sans autre si la personne n'a pas encore voté (état = "pas_voté").
Par contre, si un vote est en cours, potentiel ou effectué, une résolution doit être préalablement demandée à xVote. Celui-ci va automatiquement verrouiller l'état, abandonner les éventuelles actions en cours, révoquer un possible droit de vote; ou, le cas échéant, il va -et avec l'aide de la scrutation, qui journalisera l'acte- détruire un bulletin scellé déjà déposé[5]. À la suite de cette requête à xVote, l'état de vote est passé à "bloqué" et la fiche de l'ex-électeur peut être supprimée.

La résolution d'une réclamation (p.ex. pas reçu/perdu la carte de vote, une panne d'ordinateur, une coupure de liaison internet), soit en conséquence la requête d'une nouvelle carte de vote (donc, de nouveaux codes internet NI, MP et NA), peut se faire immédiatement si l'électeur n'a pas encore commencé une opération de vote. (état="pas_voté").
Dans le cas contraire, une résolution doit être préalablement demandée à xVote. Si l'électeur n'a pas encore déposé de bulletin, xVote va automatiquement abandonner une éventuelle action d'habilitation en cours ou révoquer un possible droit de vote non encore utilisé, à la suite de cette résolution d'xVote, l'état de vote est passé à "bloqué" et la fiche peut recevoir les nouveaux codes internet et être imprimée. Sinon, c'est qu'un bulletin a déjà été déposé et l'état du vote l'indiquera.

Pour information, le détail des processus internes se trouve dans un autre document : 20070215_1605 titré "Mutations, résolution des conflits, réclamations et contestations".

En fin de session de votation

Les communes font usuellement un relevé des codes-barres par douchette lors du dépouillement anticipé (ouverture des enveloppes de transmission).
Cette lecture doit être confrontée à l'état du vote, et provoquer le cas échéant une mise à jour de celui-ci (ou sinon un rejet du vote).

En général, les communes font une saisie aussi par lecture du code-barre de la carte du citoyen se présentant le dimanche au local de vote.
Là aussi, cette lecture doit être confrontée à l'état du vote, et provoquer le cas échéant une mise à jour de celui-ci (ou sinon un rejet du vote).

5 Ceci selon les dispositions fédérales (et cantonales) concernant les droits politiques.

Si le raccordement à l'Internet/intranet n'est localement pas possible, un téléphone mobile (smartphone) à appareil photo et liaison internet mobile (GPRS/EDGE/UMTS) est suffisant; alternativement, la carte de vote peut être spécialement adaptée (masque grattable/arrachable).

Si l'état est zéro (n'a pas encore voté) la mutation de l'état doit être exclusive et atomique avec la vérification préalable de la condition.

Une tentative de vote doit être refusée s'il y a déjà eu un vote papier.

Dans les autres cas relevant du vote par Internet, la situation de conflit doit subir une résolution. Elle est décrite en détail dans un autre document : 20070215_1605 titré "Mutations, résolution des conflits, réclamations et contestations".
La résolution utilise la clef (du facteur) de masquage, qui est sécurisée dans une unité matérielle scellée distincte des serveurs d'xVote; les bulletins éventuellement traités sont encore chiffrés, et après retraits ils sont non seulement détruits, mais indéchiffrables même après dépouillement de l'urne (la clef de déchiffrement reste inaccessible).

La résolution des cas de potentielle tentative de double vote (papier ou précédent vote Internet parfait -après résolution par xVote) est hors du domaine de ce document, car il s'agit d'un délit.

Ouverture de l'Urne

Lors de clôture du scrutin, avec le rassemblement des scrutateurs, les rapports[6] des opérations du service de scrutation, de celui d'Habilitation et de l'urne sont vérifiés et comparés. Les éventuelles opérations de corrections administratives (retraits de bulletins) ayant impliqué la scrutation, et en particulier employé la clef du facteur de masquage, doivent être justifiés par l'Administration aux scrutateurs.

Les conditions suivantes peuvent être vérifiées, le cas échéant automatiquement::

- que le nombre de bulletins reçus par la scrutation est strictement égal au nombre de bulletins trouvés dans l'urne (outre les cas de retraits);
- que le nombre[7] d'estampilles délivrées par la Scrutation est égal au nombre d'habilitations effectuées;
- que ce nombre est légèrement supérieur ou égal au nombre de bulletins dans l'urne;
- que toutes les estampilles des bulletins de l'urne sont correctement validées par l'Habilitation;
- que leurs clefs se trouvent dans la liste de la Scrutation;
- que les signatures par la Scrutation de tous les descripteurs des bulletins sont valides;

6 Les résumés automatiques des journaux. Les rapports sont extraits par des clauses des bases de données textuelles formant les journaux. Ces derniers sont constitués d'inscriptions structurées numérotées, horodatées et signées (objets numériques de confiance).

7 Strictement, identique pour les phases 3 d'habilitation complètes, sans interruption à la signature de la carte, c-à-d. (pour l'application cliente originale ou identique, hors rupture) identique au nombre de paquets de votes déposés. Sinon légèrement supérieur. Les traces des opérations dans les journaux de l'Habilitation et de la Scrutation permettent, le cas échéant, de lever le doute.

- que la séquentialité[8] des bulletins dans l'Urne est exacte[9], tant au travers de leurs numéros d'ordre que du lien de succession;
- que la séquentialité correspond à celle des récépissés[10] reçus par la Scrutation;
- que tous les récépissés reçus par la scrutation ont leur bulletin correspondants dans l'Urne:

Les scrutateurs présents, au moins le quorum[11] minimal, insèrent et libèrent leurs éléments de la clef privée de l'Urne. Avec la donnée de la portion de l'Administration, la recomposition de la clef peut être opérée au sein du module de sécurité, et les bulletins sont déchiffrés (du domaine ou État -canton).

Avec le dépouillement, soit le déchiffrement des bulletins, l'intégrité et l'authenticité (du contenu) de chaque bulletin sont vérifiées par le sceau de leurs estampilles, c'est-à-dire la signature par leurs clefs anonymes dument validées.

Réception des résultats du vote

À l'issue du dépouillement, l'informatique cantonale reçoit un fichier avec :

- le relevé du nombre total de droits de vote délivrés,
- de bulletins correctement reçus et attribués[12],
- du nombre total de bulletins traités (valables)
- du nombre total de nuls[13];

puis commune par commune (ou plus exactement par circonscription électorale)

- du nombre[14] de bulletins traités
- du nombre de bulletins nuls,

8 Les bulletins reçus par la Scrutation sont enregistrés, puis envoyés (avec une gigue aléatoire) à l'Urne, ils sont signés avec un numéro d'ordre d'envoi par la Scrutation, et comportent la trace de la clef anonyme du bulletin précédent.

9 En cas de retrait, le descripteur est maintenu, seul le bulletin est enlevé.

10 Les bulletins reçus par l'Urne sont horodatés et un récépissé (avec trace) signé et remis à la Scrutation.

11 En cas de défaut, ou d'insuffisance, des scrutateurs, et sur ordre de l'Autorité supérieure, l'élément de reconstruction (de la clef privée) dissocié entre ceux-ci, et qui a été aussi maintenu entier, scellé, signé par eux et notarié, est utilisé. L'autre élément est dupliqué et remis à deux officiers administratifs distincts. Il y a ainsi deux (fois deux) moyens de reconstitution de la clef de déchiffrement. Les éléments de clef (privée) sont détruits après reconstruction.

12 Un citoyen utilisant un logiciel tiers pervers, mais respectant strictement le protocole des transactions, pourrait remettre un bulletin dans un envoi bien formé, mais dont la circonscription électorale est fausse (pas celle du citoyen).
Le droit de vote ayant été falsifié, la tentative de fraude est détectée, le bulletin -encore verrouillé- est écarté et non versé dans l'urne (considéré comme non reçu).
► Dans le vote papier, cela équivaut à modifier la carte de transmission, et à envoyer son vote au greffe municipal d'une autre commune.

13 Un citoyen utilisant un logiciel tiers pervers, respectant strictement le protocole des transactions, pourrait remettre un bulletin bien arrivé, correctement attribué, mais intraitable après dépouillement : indéchiffrable (mal chiffré), incompatible (mal formé), invalide (mauvaises valeurs), inapproprié (fausse circonscription), inadéquat (faux droits de vote), irrecevable (signature erronée).
► Dans le vote papier, cela équivaut à avoir une carte de transmission correcte, mais un bulletin (dans l'enveloppe de vote scellée) inacceptable : annoté, gribouillé, multiple, mal rempli (p.ex. oui+non), étranger, corrigé ou sur un support non officiel.

14 La somme des bulletins traités de chaque commune est égale au nombre total de bulletins traités, de même la somme des nuls de chaque commune est égale au total des bulletins nuls. Lors d'une votation, pour chaque question d'une commune, la somme de oui, de non et de blancs est toujours égale au nombre de bulletins traités (valables) pour cette commune.

et -pour une votation- pour chaque question

- le nombre[15] de oui, de non et de blancs,

ou -pour une élection- pour chaque fonction électorale,

- la liste des candidats avec le total de chacun
- et -le cas échéant- les totaux des listes (la neutre et les nominales).

Il est à remarquer que, si le citoyen utilise le logiciel authentique (ou un homologue[16] de qualité), son bulletin est toujours valide, l'attribution, les droits et toutes les questions le sont. Il ne peut pas y avoir de cas de nullité.

Après la session de votation

Le registre est maintenu durant la période de recours. Les clefs de constructions de vote ont été détruites.

Les contestations peuvent être intégralement résolues soit par les enregistrements dans le Registre des Électeurs, les listes de la Scrutation, les traces des opérations dans les journaux (des serveurs d'xVote), en particulier par l'ensemble des éléments horodatés et cryptographiquement signés.

Le contenu de l'Urne, les bulletins estampillés (signés), est intégralement vérifiable et revérifiable, y compris par des logiciels tiers.

> Le cas particulier de la contestation sur la bonne réception/intégration du vote d'un citoyen est décrit en détail dans un autre document : 20070215_1605 titré "Mutations, résolution des conflits, réclamations et contestations". La résolution doit être opérée avec la participation du citoyen contestant, car la clef de masquage a été détruite (les bulletins sont désormais en clair).
> L'électeur contestant doit se présenter[17] au service des votations avec son identité numérique, il opère seul sur un poste isolé muni de l'accès authentifié aux serveurs xVote. L'application du poste vérifie l'identité numérique et la qualité d'électeur ayant voté, et -à l'aide de la clef privée de l'identité numérique, de valeurs chiffrées dans le R.E et de celles mémorisées par la Scrutation- elle extrait de l'Urne dépouillée le bulletin de vote, le vérifie et l'affiche.
> *Il est à souligner que cette résolution n'a pas beaucoup de sens en elle-même, car, entre le contrôle que peut faire l'électeur lui-même (récépissé) et le contrôle qui est fait par la commission électorale du contenu de l'Urne et des bulletins dépouillés, toutes les preuves de bonne fin sont déjà acquises. Il pourrait s'agir ici d'un moyen de vérification d'ordre moral ou de qualification sur des bulletins surnuméraires.*

À l'issue de cette période, le R.E. est détruit. Il en est de même des journaux et mémorisations des serveurs d'xVote, de leurs sauvegardes, des clefs restantes ou parties restantes de clefs.

---

15 Ou, le cas échéant, initiative et contre-projet.

16 Le protocole de vote et les processus des serveurs sont prévus pour accueillir tout client fonctionnant correctement, l'original ou un homologue valide. Une application cliente malveillante verrait sa production obligatoirement détectée et refusée à un stade ou l'autre du déroulement, au plus tard lors du dépouillement (bulletin nul).

17 L'électeur peut toujours, à tout moment et depuis chez lui, vérifier que son *bulletin* a bien été déposé dans l'urne (phase 5 : contrôle du processus de vote) en validant le récépissé que celle-ci a fourni. Le cas ici est s'il veut vérifier le *contenu* du bulletin. Il ne peut le faire en autonomie, car alors il disposerait d'une *preuve* de la teneur de son vote (le bulletin est authentifié), autrement dit d'une possibilité de vente de sa voix.