Introduction

Ce document présente de manière générale la relation entre xVote et l'informatique cantonale, (dans l'introduction), puis de manière précise dans la section suivante.

Il montre que l'adaptation de l'informatique cantonale à xVote est très restreinte, et précisément définie.

La partie propre à la relation avec l'Administration cantonale (surtout le service "Institution") est couverte dans le document de titre "Relations entre l'administration cantonale et xVote" et de nom "20070221_1507".

La définition du contenu du Registre des Électeurs se trouve dans le document de titre "Description du Registre des Électeurs" et de nom "20060111_1526".

Périmètre couvert par xVote :

xVote traite la totalité du cycle du vote par Internet depuis le **Registre des Électeurs** constitué par le canton (p.ex. pour Vaud, il s'agit de la fonction première de VotElec qui collationne ces données), soit :

- la création des diverses clefs cryptographiques de la session, dont la clef[1] de l'urne avec sa partie déchiffrante neutralisée jusqu'à la clôture;
- l'établissement des champs personnels[2] liés au vote par Internet, de la carte de vote;
- la gestion de la détermination[3] (ou inscription) du citoyen de recevoir sa carte de vote par Internet (ou à défaut par voie papier traditionnelle);
- l'envoi[4] sécurisé de la carte dématérialisée en remplacement de la carte/liasse papier envoyée par la poste, ceci pour les citoyens ayant utilisé précédemment le vote par Internet et ayant opté pour cette méthode;
- le remplissage de la carte de vote dématérialisée, signature -numérique- et retour sécurisé;
- la constitution du bulletin, envoyé de manière sécurisée;
- le remplissage, l'authentification du droit de vote et le scellement;
- le chiffrement du bulletin et son retour sécurisé à l'urne;
- la mise à jour du registre des électeurs pour le vote par internet;
- la gestion des conflits potentiels entre les mutations du registre des électeurs et

1 Propre au canton (K_U^{dom})

2 Il s'agit des champs Numéro d'Identification (NI, alphanumériques majuscules), Mots de Passe (MP, six courtes chaines alphabétiques) et Nombre Authentifiant (NA, chiffres, lettres majuscules et minuscules, caractères spéciaux).

3 Les indications proviennent du service d'identité numérique, elles sont donc de fait conservées d'une session à l'autre.

4 Le serveur SMTP devrait être celui du canton, pour permettre la vérification de l'expéditeur (corrélation avec adresse du champ "FROM"). Il est souhaitable que le service offre les moyens de contrôle "Sender Policy Framework /SPF" (dans son serveur DNS, RFC 4408) et/ou "DomainKeys Identified Mail /DKIM" (Yahoo, en cours normalisation IETF).

l'état du vote par internet;
- la résolution des contestations pour le vote par internet;
- l'information sur la situation du vote par internet et les alarmes éventuelles durant la session;
- le dépouillement pour le vote par internet.

jusqu'au retour des **résultats** par commune (nombre de réponses pour chaque question) à l'informatique cantonale (p.ex., pour Vaud c'est la fonction seconde de VotElec qui reçoit ces résultats, pour le Valais c'est le système mis en place par le webmaster de l'I-VS -service d'information du Valais- qui effectue cette fonction).

Il est à noter que toutes les données nécessaires pour les statistiques se trouvent dans le R.E. à l'issue de la session; ceci bien sûr sans possibilité de lien avec le bulletin dans l'Urne et son contenu.

Point important

Le système xVote ne nécessite **aucune mémorisation d'une session à l'autre** de la part de l'informatique cantonale (ou municipale) :

- Le système xVote laisse en permanence la liberté de choix aux citoyens et citoyennes, **il n'y a pas d'inscription, et à fortiori pas de désinscription, pour voter ou non par Internet.** À chaque session, dès que le citoyen ou la citoyenne a reçu son matériel[5] de vote, il ou elle peut librement choisir sa manière de voter sans la moindre démarche préalable.
- Le système xVote **donne la possibilité[6] d'éviter l'envoi par l'État du matériel de vote papier par la poste aux citoyens et citoyennes** votant par Internet.
  Dans ce cas, le système xVote détermine -durant les préparatifs précédant une session de votation- quels citoyens et citoyennes doivent recevoir la liasse papier (et donc l'indication d'impression de celle-ci) et effectue la préparation et l'envoi des liasses dématérialisées de manière totalement automatique, personnelle et absolument sécurisée, pour ceux ayant opté pour ce service.
  Toujours dans ce cas de figure, le système xVote **prend à sa charge et de manière simple et naturelle l'inscription et la désinscription sécurisée** (et le contrôle de validité) **pour la réception du matériel de vote dématérialisé** par les citoyens et citoyennes qui le désirent. La conservation, et les mutations, des données nécessaires (volonté de recevoir et adresse) sont déléguées au système xID d'infrastructure à clef publique (PKI) pour l'identité numérique.

5 Le matériel peut avoir été reçu sous la forme papier, comme sous la forme dématérialisée. Dans ce dernier cas, il suffit à l'électeur d'imprimer sa carte pour voter traditionnellement (la carte est disponible indirectement en [Adobe Acrobat] Portable Document Format -PDF).

6 Pour les titulaires d'une identité numérique de classe '1', aucun envoi n'est strictement nécessaire, car le vote se fait sans opération d'identification/authentification autre que l'utilisation de l'identité numérique. Pour les titulaires d'une identité numérique de classe '2' (celle obtenue par la votation), un complément d'identification est périodiquement nécessaire, qui permet un renouvèlement régulier souhaitable. La réception de la liasse de vote papier ou (plus confortable) par courriel permet de renforcer périodiquement la qualité de l'identité en assurant que serait détectées les captations (par absence suite au détournement du courrier) ou piratage (par tentative de doublet du renouvèlement), ou inversement en provoquant l'obsolescence d'une possible identité falsifiée.

Données entrée/sortie

En entrée xVote prend les données dans le **Registre des Électeurs.**

Trois informations supplémentaires doivent s'y trouver :

- la date de naissance,
- la(les) commune(s) d'origine (pour les citoyens suisses),
- le nouveau numéro d'assurance sociale (NNAS).

Quelques champs doivent être créés vides pour les informations retournées par xVote.

xVote ne conserve aucune donnée nominale.
Le système complémentaire xID d'identité numérique, ou architecture à clef publique (PKI) conserve certaines données, dans le cadre usuel de la gestion standard de l'identité numérique et ceci selon l'obligation des prescriptions légales.

En sortie, soit à l'issue de la votation, xVote fournit un fichier XML, avec les résultats ventilés par commune et (au sein de chaque commune) pour chaque question ou choix (pour le vote ou l'élection).

Technologies requises

xVote assume l'existence d'un système de gestion de bases de données relationnelles[7] (SGBD-R) pour le **Registre des Électeurs (R.E.)**, dont la cohérence (plausibilité) des données a été réalisée.

Le système doit être atteignable par des requêtes standards au moyen d'un connecteur[8] ADO.NET/dotNET propre au système[9]. Il doit être accessible via un lien sécurisé (p.ex. VPN) depuis la grappe d'Habilitation d'xVote.

Pour garantir la cohérence des données (contraintes, ou validité des ensembles de valeurs et des successions d'état licites) dans la base elle-même, le mieux serait d'avoir des procédures enregistrées pour les mutations. Mais ce n'est pas nécessaire (voir plus bas : libertés du R.E.).

Pour l'initialisation, durant la session de vote et durant la période de recours, les fonctions de xVote sont activées, par exemple manuellement depuis l'intérieur de simples pages HTML (web forms), par des requêtes HTTPS directement adressées au serveur de l'Habilitation (nom du site comme pour le vote -domaine- et nom de la "page" selon l'ordre) ou en les incluant dans des développements ad hoc (accès SOAP).

Libertés du Registre des Électeurs

Le cœur d'xVote (dans la grappe d'Habilitation) accède au R.E. via une couche d'isolation (script interne) propre à chaque domaine (ou canton). De ce fait, l'existence ou non de procédures enregistrées, leurs noms et paramètres, ainsi que le choix des noms de champs est libre.

7 Strictement, il n'est pas nécessaire que la base soit relationnelle.
8 Des connecteurs sont donnés disponibles pour les SGBD-R suivants : PostgreSQL, MySQL, Firebird Interbase, SQLite, Oracle, Sybase, DB2, Microsoft SQL Server, Progress RDBMS, Mimer SQL.
9 … ou à défaut d'un pilote ODBC, mais ce n'est pas encouragé. Dans ce cas, les requêtes sont SQL/CLI.

En amont durant les préparatifs de la votation :

L'informatique cantonale (VD : VotElec) constitue le **Registre des Électeurs** par consolidation des extraits des registres communaux.

Il faut aussi collecter (obtenir des extractions faites par les communes) trois informations supplémentaires :

- la date de naissance;
- la/les commune(s) d'origine(s) pour les citoyens suisses, ou assimilé (lieu d'origine/naissance) pour les étrangers;
- le numéro unique d'identification (NNAS).

Quelques champs doivent être définis (créés) dans la base représentant le registre pour les informations retournées par xVote et utilisées jusqu'à la clôture de la votation (voir dernière partie de ce document).

Le canton (l'informatique cantonale, l'éditique) est déchargé de la préparation de la carte/liasse papier à envoyer par la poste pour les citoyens ayant utilisé précédemment le vote par Internet et ayant opté alors pour la carte de vote dématérialisée, car xVote prend intégralement en charge la demande, et, en remplacement du papier, sa préparation et son envoi par courriel sécurisé.
La chaine de traitement de l'éditique ne doit donc imprimer et envoyer la liasse que pour les citoyens restants (le Registre des Électeurs contient cette indication).

Sur la carte de vote papier, l'impression actuelle (nom, adresse, etc.) doit être complétée par les trois champs supplémentaires :

- numéro d'identification (10 positions alphanumériques -cinq groupes de deux- majuscules),
- mots de passe (6 petits mots de max. 8 lettres[10] minuscules -pour le français : de trois lettres[11]),
- nombre authentifiant (12 positions -quatre groupes de trois- lettres majuscules et minuscules, chiffres et quelques caractères spéciaux courants).

Ces valeurs se trouvent (au format chaines de caractères) directement dans le Registre des Électeurs, introduits par xVote lors de l'initialisation du Registre.

En aval, à l'issue de la votation :

L'informatique cantonale (VD : VotElec) reçoit d'xVote un fichier XML, avec les résultats par commune, et pour chaque question[12] le nombre de réponses oui/non/blanc ou -le cas échéant- initiative/contre-projet/blanc (pour les votations) et/ou pour chaque fonction élective le nombre de voix par élus et -le cas échéant- par liste (pour une élection).

Le fonctionnement se fait donc comme actuellement, mais avec une seconde source dont les données s'ajoutent aux premières (les communes et leur bureau électoral).

10 En minuscule et avec accents selon l'usage, mais en fait, ni la casse ni les signes diacritiques ne sont pertinents.

11 Chaque mot code un octet, soit 256 valeurs. Dans une langue donnée, il faut donc avoir une liste de 256 mots distincts, simples à lire et écrire pour les électeurs. En français, il existe une telle liste de mots limités à trois lettres (tirée de l'Officiel du SCRABBLE™, Larousse 2003).

12 Il y a aussi le nombre de bulletins nuls (entiers), pour le cas où une application client frauduleuse ou erronée aurait été programmée et utilisée.
Voir la section "Réception des résultats du vote" du document de titre "Relations entre l'administration cantonale et xVote" nom 20070221_1507.

Durant la votation, ainsi qu'en amont et en aval :

xVote prend ses données (ou fournit ses mises à jour) dans le **Registre des Électeurs**; il est assumé un SGBD(-R), atteignable via des requêtes effectuées par un "provider" dotNET/Mono (ADO.Net)[13].

Il s'agit essentiellement de deux types de requêtes : à partir d'une clef (secondaire) obtenir un enregistrement, écrire (certains champs) d'un enregistrement déterminé par une clef (primaire).

La base doit avoir comme clef primaire le Numéro d'Électeur (NE, dit aussi numéro de carte, NC), et comme clefs secondaires (uniques, clefs candidates) le Numéro d'Identification (internet, NI) et le Nouveau Numéro d'Assurance Sociale (NNAS).

Généralités :

Les fonctions administratives d'xVote sont activées par des requêtes HTTPS (Web Forms).

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

Optionnellement, l'informatique cantonale pourrait offrir, durant la votation, une interface unifiée au registre électoral pour la gestion par les communes des mouvements ou réclamations des électeurs.

> Les réalisations des fonctions d'xVote se font au moyen de requêtes Web sécurisées (HTTPS) au système, avec authentification croisée (et chiffrement). Optionnellement, elles peuvent être placées dans des pages interactives (HTML, Web Forms) ou dans une application ad hoc

Le Registre des Électeurs doit être conservé et accessible par xVote depuis les préparatifs -pour les initialisations- jusqu'à la fin de la période de recours -pour la résolution des éventuelles contestations.

Toutes les opérations sur le R.E. implantées par le service informatique, agissant durant la session de vote et qui sont conditionnées par, ou qui manipulent, la valeur du champ "État du vote", doivent être atomiques (en exclusion de toutes autres mutations concurrentes).

13 Il existe un tel connecteur pour la majorité* des SGBDr (sinon l'emploi d'un connecteur générique ODBC pourrait être possible).
*) PostgreSQL, SQLite, Firebird Interbase, MySQL, MimerSQL, Oracle (8i, 9i, 10g), MS-SQL Server (7.0, 2000, 2005, ult.), Sybase (ASE 12.0 et ult.),