Informations et zones de données nécessaires pour xVote dans le Registre des Électeurs

Droits d'accès :

Le SGBDr du registre des électeurs doit permettre la lecture par xVote de tous les champs utilisés :

- l'identificateur unique (NNAS)
- Nom(s),
- Prénom(s),
- Date de Naissance (avec sa validité),
- Circonscription;
- Numéro d'Électeur (NE),
- Langue du bulletin (langue de correspondance)
  [pour les cantons monolingues, ce champ peut-être absent, et virtualisé dans le script d'interface],
- Capacité électorale (confédération/canton/commune),
- Question (type et réponses, p.ex. "commune(s) d'origine(s)"),

et la lecture-mutation de ceux modifiés depuis le serveur d'habilitation d'xVote :

- Le jeu de questions,
- Les codes internet NI, MP et NA, et l'identifiant binaire,
- L'envoi de la carte de vote,
- La date de traitement de la carte de vote,
- L'état du vote,
- Horodate du vote,
- La carte de vote (signée en retours),
- L'agrégat binaire.

Contraintes :

Le champs NE doit être intangible (après création de la fiche).

Les champs NI, MP et NA ne doivent être modifiables que par xVote (initialement "null"), de même pour l'identifiant binaire et l'agrégat binaire (qui n'ont de sens d'être lus que par xVote).

Le champ d'État du vote ne doit être modifiable que par xVote, le processus de vote papier et l'administration (mutation); seules les transitions[1] suivantes sont valides[2] :

xVote – de (0;-) à (3;0) ou (1;1),
de (1;n) à (1;m) pour $0<n<m$,
ou de (1;n) à (3;m) pour $0<n\leq m$,
év. les transitions du vote papier et/ou de l'administration.

1 Le premier élément (mode) peut aussi être transitoirement négatif : (-3;x), à titre de sémaphore bloquant.

2 La contrainte peut être ou non vérifiée par le SGBD. Elle peut-être, par exemple, contrôlée au moyen d'une mutation se faisant exclusivement par appel de procédure enregistrée.

vote papier – de (0;-) à (2;x) pour x quelconque,
de (3;n) à (2;x) pour n et x quelconques

administration - de (m;n) à (3;0) pour m et n quelconques,
de (3;0) à (0;-).

Les lectures+mutations du champ d'Etat du vote, ou d'une manière générale les mutations dépendant conditionnellement de l'état du champ, doivent impérativement être atomiques *.

*) le couple d'opérations n'est pas interruptible, le test d'état et la suppression sont exécutés monolithiquement, en exclusion de tout autre mutation concurrente. Il ne s'agit pas de la propriété d'*A*CID.

Charge :

Le SGBDr doit supporter la charge du vote par internet, typiquement en crête la dernière semaine de la session, et surtout en début de soirée.
Prévoir une augmentation de la participation de 10% (c-à-d. typiquement 60%), et un taux d'usage internet pouvant aller de 40% à 70%.des votes.

Le SGBDr doit supporter la crête d'accès du dépouillement anticipé (ou pré-dépouillement) des votes par correspondance dans les communes (contrôle de l'état de vote et sa mutation).
Actuellement il s'agit de 80-95% des votes, traités le ou les pénultième(s) ou antépénultième(s) jours de la session.

Il en sera de même pour le contrôle d'entrée dans le local de vote (état=2), mais vraisemblablement avec beaucoup moins de concentration du nombre de requêtes.
Actuellement 5-20% des votes, seulement le dernier matin, ou complété par un créneau horaire l'avant-dernier jour de la session.

Généralités

La connexion d'xVote avec le Registre des Électeurs se fait par un connecteur ADO.NET (dotNET) et une liaison sécurisée.

Les identificateurs (noms des tables, des colonnes, etc.) ne sont pas fixés ici, ils sont configurables.

Les types[3] de données indiqués dans ce document sont choisis pour être SQL-universels : Les entiers peuvent en fait être stockés dans des objets plus grands que ceux indiqués (sp. les entiers isolés tynyint en smallint), mais leurs valeurs ne doivent pas être plus grandes que ce que permet la taille indiquée ici.

les entiers int = 32 bits,
smallint = 16 bits,
bigint = 64 bits,
tinyint = 8bits
avec u_* les mêmes, mais non signés;

les chaines de caractères sont Unicode (TChar sur 16bits);

3 L'indication des types est pour la compatibilité avec l'usage des SGBDr, indépendamment du fonctionnement du connecteur ADO.NET.

les chaines (de caractères, d'entiers homogènes)	sont des vecteurs de longueur fixe ou variable avec l'indication d'un maximum; elles peuvent être nulles ou pas.
les booléens	deux valeurs 0 (False/faux) ou 1 (True/vrai), usuellement sur 16 bits (similaires à u_smallint);
la date	est une structure (AAA/MM/QQ) [année : smallint, mois, quantième : u_tinyint]; l'année[4] est complète et à quatre chiffres (p.ex. 1901), le mois 1..12 et le quantième 1..31 forment une date valide : le mois (et év. l'année) détermine le quantième maximal;
l'horodate	est une structure "timestamp" (AAAA/MM/QQ HH:MM:SS.FFF) [année : smallint, mois, quantième, heure, minute, seconde : u_tinyint, fraction : u_bigint]; année, mois et quantième comme pour la structure date, heure 0..23, minute et seconde 0..59, fraction 0..999_999_999 et exprime des milliardièmes de seconde.
blob	chaine d'octets écrits ou lus en bloc, de manière contigüe, sans interprétation par la base.(aka Binary Large Object). Peut-être un chaine (fixe) de u_tinyint stricts.

Table des fiches de citoyens

Le champ "*Numéro d'électeur*" ou, le cas échéant, le couple de champs "*Commune politique index*" et "*Numéro d'électeur*", est/forment la clef primaire.

Le champ "*Numéro d'identification*" est une clef secondaire (ou clef candidate, c'est-à-dire est un second index).
Au début d'une requête de vote, xVote effectue le premier accès à la fiche du requérant d'après cette clef secondaire, et retourne le résultat sous la clef primaire.

Pour un électeur titulaire d'une identité numérique valide, la recherche a lieu à partir de l'"*Identificateur Unique*" (NNAS), qui est par essence aussi une clef secondaire (ou clef candidate, c'est-à-dire est un troisième index).

-- rempli par la consolidation des registres communaux

Identificateur Unique :	u_bigint *
Genre :	u_tinyint ou u_smallint, deux valeurs : { Masc=1, Fem=2 }

4 Pour les autres dates que de naissance, seul l'intervalle 1901..2399 est valide pour xVote.
Pour les dates de naissance (et pour xVote) :
Les années strictement inférieures à **1897** sont rejetées (donc la fiche de l'électeur aussi).
Les dates strictement supérieures à la date courante sont rejetées (donc la fiche de l'électeur aussi).
Les années inférieures à 1901 sont assimilées dans xVote a cette dernière (1897-1900 ne sont pas bissextiles) .
Seules les années comprises entre 1901 et 2399 sont traitées en interne d'xVote.
Note : doyen(ne) actuel(le) mondial(le) : Yone Minagawa, née le 4 janvier 1893
Il n'y a actuellement pas de supercentenaires (110a et plus) en Suisse www.grg.org
La doyenne de Suisse est Rosa Rein née le 24 mars 1897 (réside près de Lugano)

Nom(s) :	chaine variable non nulle de caractères (max. 255 positions) ** (Il s'agit du champ "nom officiel" du contrôle des habitants)
Prénom(s) principal(aux) :	chaines variables de caractères (max. 255 positions) ** (Il s'agit normalement des "prénoms usuels" ou à défaut des "prénoms officiels", le champ peut-être vide selon la norme)
Date de naissance :	date (voir le champ "Validité DdN") L'année devrait être comprise entre 1897 et 2399, la date doit être antérieure au scrutin. (les dates antérieures au minimum de traitement -1901- seront silencieusement assimilées par xVote à celui-ci)
Validité DdN :	u_smallint { 0=entière, 1=mois_année, 2=année_seule } (Si le quantième est inconnu, la valeur correspondante dans la DdN est ignorée; si le mois est aussi inconnu, seule l'année est prise en compte)
Circonscription :	u_int (non nul) index (clef étrangère) dans la table des communes politiques du canton (ou plutôt et plus généralement des circonscriptions électorales)
Numéro d'électeur :	(NE) chaine variable non nulle max 64 positions, définit univoquement la personne (pendant la session), le cas échéant en combinaison avec le numéro de circonscription (c'est le numéro de carte NC inscrit en code-barre sur celle-ci).
Langue du bulletin :	chaine nulle ou fixe à deux positions. (Il s'agit du champ de "Langue de correspondance", selon le mode standard en codage ISO 639-1, nulle pour la langue par défaut). [Le script d'interface interprète la langue par défaut, selon la configuration du domaine, et virtualise celle-ci pour les cantons monolingues, où ce champ peut-être absent]
Capacité électorale pour Confédération, Canton, Commune :	trois booléens { False=0, True=1 } ne doivent pas être tous zéro
Type de Question :	u_smallint { commune_d_origine=0, ... }
Réponses :	vecteur variable non nul max 32 d'index valide(s) (u_int non nul, clefs étrangères) dans la table de questions adéquates (p.ex. citoyen suisse = index de sa / de ses communes d'origine(s))

Éventuellement, l'adresse postale pourrait être aussi présente (de toute façon, elle l'est pour l'envoi postal par l'éditique), et serait alors utilisée pour la gestion de l'identité numérique.

(*) note : Nouveau Numéro d'Assurance Sociale, à 13 chiffres, le passage progressif entre ancien numéro AVS et nouveau a lieu en 2007, le

nouveau sera définitivement utilisé à partir de 2008.
l''Identificateur Unique'' de la personne est par principe le seul moyen de lier une identité numérique avec son porteur, pour l'usage des processus informatiques personnalisés. La structure sous-jacente de l'identité numérique (clefs, certificat) étant obligatoirement renouvelée périodiquement (donc son identificateur ou numéro change), le lien avec son porteur est maintenu (confidentiellement et pour l'État) par le service de gestion des identités (autorité de certification) au moyen de cet ''Identificateur Unique''.
S'il n'y avait pas d'identificateur unique pour une personne, le vote pourrait avoir valablement lieu (le numéro d'électeur est enregistré pour l'identification temporaire), mais l'identité numérique ne pourrait pas être utilisée pour les votes ultérieurs (nécessitant une ré-identification complète à chaque fois), et en particulier l'envoi de la carte de vote dématérialisée ne serait pas possible.

(**) note : Dans le cas où un certificat X509 est émis (mais pas pour une signature de clef openPGP) et pour des raisons de norme X509, le nom et le prénom sont enregistrés agrégés dans le certificat et avec une longueur totale de seulement 64 caractères. Au minimum, figurent dans le certificat au moins le premier élément du nom ou le maximum possible avec le premier prénom, le cas échéant avec troncature.

-- rempli par les serveurs d'xVote durant les préparatifs

Les NI, MP et NA sont pour permettre l'impression des cartes (les codes détecteurs d'erreur sont compris). xVote utilise pour son traitement l'identifiant binaire.

Questions :	vecteur variable de longueur max 64 d'index (u_smallint) (clefs étrangères) dans la table ad-hoc
Numéro d'identification :	(NI) chaine fixe de 10 caractères alphanumériques (majuscules); dix chiffres en base trente-deux, les deux derniers forment un CRC-10
Mots de passe :	(MP) 6 chaînes variables max. 8 positions; six petits mots (en français de trois lettres) figurant chacun un octet, le sixième est un CRC-8.
Nombre authentifiant :	(NA) chaine fixe de 12 caractères (alphanum. min/maj. et certains spéciaux); douze chiffres en base soixante-quatre, les deux derniers forment un CRC-12
Identifiant binaire :	chaine fixe de trois u_bigint (3x8 octets, strictement 5, 5, 7½) Version binaire des trois précédents champs.

Envoi carte de vote : u_tinyint initialisé à zéro
{ 0 = non (init.),
1 = impossible_par_courriel_identification_invalide,
2 = impossible_par_courriel_adresse_rejetée,
3 = envoi_par_poste,
4 = possible_par_courriel (adresse et identification val.),
5 = échec_courriel_certificat_invalide,
6 = échec_courriel_adresse_rejetée,
7 = effectué_par_courriel (adresse et certificat valides)
}

Date de traitement de la carte : structure horodate* (initialisée à nul)

(*) note : tenue à jour par xVote pour les valeurs '1', '2', '4' à '7' du champs "Envoi_carte_de_vote", peut être tenue à jour par l'informatique cantonale pour sa valeur '3'

-- maintenu durant la votation

Note : Lors d'une tentative d'un vote papier, l'état doit être antérieurement à "pas_voté" ou '0' et passer à "a_voté_autrement"=2, avec le mode au choix du canton.
L'opération de contrôle et mutation conditionnelle doit être atomique (et donc exclusive).
Pour les cas de conflits[5] (état antérieur à 1="a_voté_internet"), après la résolution par xVote, l'état doit être à "bloqué" ou '3' pour être muté.

État du Vote : deux tinyint init. resp. à trois et à zéro
Premier entier -
Mode : { 0 = pas_voté (init.),
1 = a_voté_internet,
2 = a_voté_autrement
3 = bloqué (transitoire)
}
la valeur peut être transitoirement négative (sémaphore)
Second entier -
Étape[6] (INet) : { 1 = demande_vote_en cours
(verrou durant l'habilitation),
2 = a_reçu_droit_vote
(estampille délivrée),
3 = a_envoyé_vote,
(transitoire, bulletin à la scrutation)
4 = a_voté
(contrôlé, bulletin transmis à l'urne)
}
ou
Moyen (autre) : { 1 = au_local (p.ex.),
2 = par_correspondance (p.ex.),

5 Voir le document : 20070215_1605 titré "Mutations, résolution des conflits, réclamations et contestations"
6 Le Mode "Bloqué"=3 partage l'intervalle des valeurs "Étape" (ici en fait Étape_précédente) avec "Mode"="à_voté_internet", mais avec en plus la valeur primaire 0="pas_encore_voté".

3 = ...
}

Horodate du Vote :	structure horodate, nulle originellement; puis moment d'enregistrement des états (étapes pour xVote).
Carte de Vote	chaîne variable max. 3584 car. (7 Ko), init. nulle.
Agrégat binaire :	un blob de 768 octets ou ¾ Ko La structure contenant la clef anonyme publique masquée (1024 bits), le facteur de masquage chiffré (symétrique, 1024 bits), la signature binaire des deux valeurs par les scrutateurs (2048 bits) et la clef anonymes (priv+pub) chiffrée sous la clef identitaire (2048 bits).

L"Endianess" (boutianité) des suites d'octets figurant de grands nombres entiers suit la norme "Network Byte Order", soit est "Big-Endian" (grosboutien).

Table des circonscriptions électorales du canton

Définit les clefs de validation des estampilles, permet -le cas échéant- de séparer les bureaux de vote d'une même (grande) commune.

Index :	u_int non nul (clef primaire)
Identificateur communal :	u_int non nul (clef étrangère dans la table ci-dessous)*

Table des communes politiques suisses (table de questions 0)

Index :	u_int non nul (clef primaire)*
Nom :	chaine variable max. 255 positions** et ***

Autres Tables de questions (n >= 1)

Index :	u_int non nul (clef primaire)
Nom :	chaine variable max 255 positions

(*) note : il s'agit de l'identificateur unique des communes suisses, tel que géré par l'OFS.

(**) note : la norme eCH-0007 indique que le nom de commune est stocké sur seulement 50 caractères, calés à gauche.

(***) note : pour être inclus dans le certificat (communes du canton), il devrait s'agir du nom officiel OFS.