Papier de position

Vote électronique

Auteur: Guillau
guillau

Périmètre:

Le présent papier de position s'inscrit dans la démarche de l'exercice des droits politiques et de son exetension à l'usage de la sphère numérique. Il s'appuit sur la doctrine régissant le vote en Suisse, et son approche de l'établissement de la confiance. Le document n'abordera que les mécanismes de vote électronique numériques.

Synthèse :

Les exigences principales de ce papier de positions sont:

1. L'administration et la gestion du vote sont des tâches régaliennes de l'État et ne peuvent être déléguées à des opérateurs privés
2. Le code source de la plateforme e-voting doit être accessible en mode opensource sans aucune restriction
3. La transparence de l'ensemble des procédures de la gestion du vote électronique avec la vérifiabilité individuelle et universelle du vote
4. La mise en place d'un programme de sécurité informatique pour permettre à la population de se protéger afin de préserver la sécurité et l'intégrité de leurs moyens informatiques pour permettre l'exécution d'un vote électronique en toutes sécurité et confiance

Table des matières

Introduction:

Aujourd'hui, le vote peut s'exercer de trois manières:

- Le vote physique avec dépôt dans l'urne, après un passage à l'isoloir
- Le vote physique par correspondance, où le votant renvoit son bulletin de vote par la poste
- Le vote électronique par correspondance, où le votant utilise une infrastructure de vote électronique via Internet

Actuellement les votants ont recours de manière massive au vote par correspondance. Ce vote est en fait également un vote par anticipation.

Selon les études, les Suisses ont adopté le scrutin par correspondance. Au milieu des années 2000, le nombre de votants utilisant le vote par correspondance a dépassé le nombre de personnes se rendant aux urnes. Selon certaines études, c'est jusqu'à 90% de la population qui vote par correspondance.

Depuis 2003, la Suisse autorise le vote électronique par correspondance dans le cadre de programmes pilotes, et des évolutions importantes ont eu lieu, durant la dernière décennie et demi:

- la vérifiabilité individuelle
- la loi sur l'ouverture du code source du système de vote électronique, mais également de l'ensemble des audits de sécurité
- la mise en place d'un environnement github accueillant le source code de la plateforme genevoise CH-Vote
- La vérification individuelle
- La vérification universelle (en beta test depuis avril 2017)

Le Parti PIrate Suisse a participé à la consultation de la Chancellerie Fédérale sur le vote électronique en 2014, et avait déjà à l'époque formulé un certain nombre de remarques, qui furent très bien accueillie par la Confédération. Cependant, avec la généralisation du vote électronique de nouveaux problèmes apparaissent. Comme par exemple avec

la plateforme de vote de suisse orientale, qui connut une fin abrupte avec la non-certification pour les élections fédérales de 2015.

Faits

Après un quart de siècle de vote par correspondance et une quinzaine d'années de vote électronique, quelques faits sont à relever:

1- Tant le vote par correspondance que le vote électronique n'ont pas eu d'influence significative sur le taux de participation
2- Le taux d'adoption des deux modes de scrutins par anticipation et correspondance ont été élevé parmi les votants
3- En 14 ans, il n'y a pas eu de cas de fraude avérée lié à l'utilisation du canal de vote électronique, alors qu'au niveau du vote papier plusieurs milliers de cas ont du être traité.
4- Lors de recomptages des votes, comme cela a eu lieu lors du référendum sur la loi sur la police, les résultats du vote électronique sont restés les mêmes alors que ceux du vote papier ont fluctués de plusieurs dizaines de voix.

Les principes fondamentaux du vote électronique

Le vote électronique n'est pas une terra incognita où il est possible de remettre en question les principes fondamentaux du vote:

- La non-répudiabilité
- L'intégrité
- La confidentialité

Pour ce faire des outils cryptographiques forts doivent être employé.

Nos exigences

- Tout système de vote électronique doit assurer la non-répudiabilité de l'acte de vote, l'intégrité de l'ensemble du processus de vote, ainsi que du contenu de l'urne, et enfin la plus importante, la confidentialité, la protection de l'opinion du

citoyen, son droit politique fondamentale sans lequel la démocratique ne pourrait pas être.

- L'utilisation de moyens cryptographiques forts ne répondant pas au traité de Wassenar quant à l'utilisation d'encryption pour des applications "civiles" étant donné que le système de vote électronique n'a pas à être exporté.

L'exercice des droits politiques, une tâche régalienne de l'Etat

La gestion de l'ensemble du système de vote est une tâche régalienne. La gestion du rôle des électeurs se fait par une entité séparée.

Nos exigences

- L'ensemble des activités de la gestion, l'administration et l'exécution du vote relève de la seule compétence publique. Aucun acteur privé ou para-étatique ne peut être impliqué dans l'exécution du vote (i.e. pas d'imprimeurs privés, pas d'opérateur informatique privé, pas de fournisseurs privés de logiciel, ni de sous-traitants privés).
- L'Etat développe, gère et exploite les infrastructures de vote électronique

L'organisation des votes

Nos exigences

- Urnes à la taille des cercles électoraux actuels avec l'implication de personnes de la commune
- Les ascesseurs et scrutateurs sont désignés dans le rôle du cercle électorale
- Le suivi et la gestion de l'urne se fait dans le cercle électoral,
- La séparation des compétences:

- La gestion du rôle des électeurs incombe au contrôle de la population,
- l'organisation du vote et la production du matériel de vote électronique incombe à la chancellerie
- Aucune de ces tâches ne peut être sous-traitée

La transparence du système de vote électronique

Nos exigences

- La transparence et l'accessibilité du code source des applications de vote électronique et de gestions de la conduite du vote sont des principes inscrits dans la loi.
- Les audits informatiques et de sécurité sont mis à disposition du public selon le principe de full disclosure

La transparence et la vérifiabilité du déroulement du vote

Nos exigences

- Pour le votant:
- Le système de vote électronique doit posséder une vérifiabilité individuelle permettant au votant de contrôler, et non de modifier, son vote
- Le système de vote électronique doit posséder une vérifiabilité universelle

- Résultats détaillés des audits disponibles sans recours à la "LIPAD"
- L'ensemble des détails et des statuts du processus d'exécution d'une votation est disponible en tout temps durant son déroulement.
- Le contenu des urnes de vote électronique, les journaux d'activité, l'ensemble des procès-verbaux sont mis en ligne et tenu à disposition de manière indéterminée.
- La mise à disposition du code source est faite dans le cadre d'une licence libre, comme par exemple une AGPL.

La sécurité du matériel informatique d votants et d infrastru d vote éle

L'Etat ne peut pas affaiblir volontairement la sécurité d infrastru et d systèmes d vote ainsi que celle du matériel informatique en maintenant secrètes d vulnérabiltiés, et failles non-corrigées.

L'Etat doit prendre un rôle a dans la prévention et l'erradication d vulnérabilités informatiques affe le matériel informatique d citoyens. Sachant que par exemple les infrastru d télécommunication ont un taux d conformance d plus d 98% (homogénéité du parc d matériel), il n' a pas d raison pour que l'Etat ne puisse pas raisonnablement être impliquer dans cet effort d longue haleine.

Nos exigences

- Dés qu'il en a connaissance, l'Etat doit partager les vulnérabilités et failles informatiques, qui sont en sa possession (acquisition d'outils "govware*, partage d'information) avec les éditeurs d logiciels et la communnauté d la sécurité informatique.
- La Confédération investit les moyens nécessaires afin d permettre la mise en place d programmes proa en matière d sécurité d l'information pour l'ensemble d citoyens.

- La Confédération et les cantons font évolué les plateformes de vote électronique de manière proactive afin de maintenir un très haut niveau de sécurité et ainsi devancer l'évolution des menaces.
- Le vote électronique n'étant pas une applications étant destinée à l'exportation, la Confédération et les cantons emploient des moyens de chiffrement fort dépassant le niveau prescrit dans les accords de Wassenar, et leurs successeurs.
- Le système de vote électronique doit employé des sous-systèmes ouverts (typiquement le kit de developpement java)