Informations pour appréhender la problématique du vote électronique en Suisse

Premièrement, la Confédération n'a pas financé l'implantation de systèmes de vote "électronique" dans le but d'en sélectionner un qui serait fourni ensuite gratuitement à l'ensemble des cantons. Le but fondamental de la Chancellerie Fédérale a été d'acquérir l'expérience de l'utilisation de ce troisième mode de vote par la population, sur le terrain. Le financement -très conséquent- des projets pilotes qui a été consenti par la Confédération est uniquement dans ce but d'analyse; les développements financés sont des "à côté" de cette démarche et ne préjugent nullement des solutions qui seront choisies par les cantons.

La Chancellerie rappelle d'ailleurs, dans ses documents, que les cantons restent libres des moyens mis en oeuvre pour l'organisation d'un vote, même fédéral, car ils sont souverains. Les cantons sont donc officiellement libres de mettre en application un autre système de vote par Internet (réponse de Hans-Urs Willy, chef de la section des droits politiques de la Chancellerie Fédérale).
L'unique contrainte est le respect de l'"Ordonnance[1] du 24 mai 1978 sur les droits politiques" (ODP), complétée le 20/09/2002 par les articles 27a - 27q concernant les essais pilotes de vote électronique, et mis à jour le 22/08/2007.

Secondement, la gratuité de ces systèmes pilotes n'est qu'un leurre. En effet, les pilotes suisses ont soit été essentiellement construits sur la base de produits commerciaux (donc payants), soit même sont formés uniquement (pour le vote) d'un produit commercial soumis à licence onéreuse. Le choix d'un tel système sera donc en conséquence subordonné à l'acquisition d'importantes licences commerciales, en plus des nécessaires adaptations en régie.

1. Les projets actuels ne sont pas développés "ex nihilo" mais sont intimement et massivement basés sur des logiciels commerciaux nécessitant des licences coûteuses pour être utilisés en production.
2. L'un des pilotes est même (pour le vote) un produit commercial complet. Un canton (ou État) qui voudrait donc reprendre un tel système devrait payer ces licences (à l'acquisition -plusieurs centaines de milliers de francs-, et annuellement pour la maintenance).
3. De surcroît, au moins un de ces pilotes est basé sur une architecture matérielle propriétaire particulière d'un fabricant (qui n'est maintenant plus commercialisée).
4. Enfin, deux de ces pilotes utilisent des cartes de vote particulièrement onéreuses, voire très coûteuses.

Il est aussi révélateur que deux des pilotes ont mené leur développement dans le plus total secret, même envers la Confédération, et le fonctionnement intime de leur système est confidentiel; quant au troisième, il utilise un logiciel couvert par le secret industriel.

De plus, aucun des pilotes n'est prêt pour les élections, et surtout aucun n'ouvre la voie (et de loin) aux pétitions, référendum et initiatives.

Même si le Conseil Fédéral s'est prononcé en mai 2006 pour son introduction dans tout le pays, la Chancellerie Fédérale a des doutes sur la maturité du procédé mis en oeuvre par

1 L'ODP est basée sur la "Loi du 17 décembre 1976 sur les droits politiques" (LDP), révisée le 21/06/2002.

les pilotes (Hans-Urs Willy, SDP/ChF, ATS 12/10/2006).

En effet, il serait illusoire de reprendre ces systèmes pilotes, car

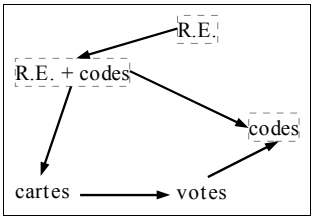
ils sont gravement déficients

pour les raisons principales suivantes.

Ces informations ont été obtenues par une analyse approfondie de ces systèmes. Les communiqués et positions officiels s'écartent largement de la réalité.

1. Aucun de ces systèmes ne répond aux conditions démocratiques, et en particulier aux prescriptions de l'ordonnance fédérale :

   - L'anonymat et le secret du vote ne sont pas maintenus :
     - ➔ Dans deux de ces systèmes, le bulletin non chiffré est livré identifié au serveur de l'Administration (le contenu est utilisé pour le filigrane d'authentification); le canal chiffré standard (TSL/SSL), seule protection utilisée, ne sert qu'à protéger le transport, il s'arrête au serveur récepteur qui possède donc en clair le contenu des bulletins.
       Par ailleurs, et de plus, la temporalité du vote (contenu des bulletins inconnu jusqu'à la clôture et le dépouillement) n'est pas respectée.
     - ➔ Dans deux de ces systèmes (autres) il y a un pseudo "brassage"[2] des bulletins (dans l'urne) par voie informatique, donc réversible et ne brouillant pas l'identification des votants [ordinateur = machine de Turing = procédé déterministe].
     - ➔ Dans les trois systèmes, il y a (possibilité de) journalisation[3] ("log") des entrées liant identités et bulletins (chaque bulletin, ou chaque classe de combinaison, possède une configuration numérique unique, donc traçable).
     - ➔ Dans l'un, le bulletin (SMS) comporte lui-même un (des) numéro(s) d'identification du citoyen.
     - ➔ Dans deux de ces systèmes, le vote se fait en s'identifiant par un numéro unique personnel se trouvant sur la carte de vote nominale.
       L'Administration a donc été (et est potentiellement[4]) en possession du lien entre le



2 En fait, une simple lecture des enregistrements de la base de donnée ("urne") dans un ordre différent de celui de l'écriture (M.Schmocker 30/10/2007).

3 Pour un des pilotes, ses responsables ont reconnu effectuer une telle journalisation de l'entrée des bulletins (au cours de la session TCP identifiée). Devant la commission des droits politiques, ils ont affirmé pouvoir utiliser le journal en cas de contestation, pour le recomptage des bulletins (Emilie Flamand, 19/05/2008).

4 Dans ces pilotes, la première base de données (ou liste) liant le nom l'électeur avec son numéro d'identification est nécessaire et ne peut être détruite, ni avant ni en clôture de scrutin.
Avant la clôture du scrutin, cette liste doit être utilisée pour résoudre les réclamations : un citoyen peut arguer avoir perdu sa carte de vote, avoir subi une panne informatique ou une perte de connexion, etc., et ainsi ne pas avoir pu effectuer ou terminer son vote et demander un nouveau droit de votre (une nouvelle carte). Il faut pouvoir partir du nom du citoyen pour vérifier la présence ou l'absence de son bulletin dans l'urne électronique*.
(*) ou au moins l'arrivée du bulletin dans le serveur frontal, avant son insertion dans l'urne, mais c'est moins probant.
Cette liste liant le nom et le numéro doit même être maintenue après la clôture du scrutin (et donc l'ouverture de

nom, le numéro et donc le bulletin de vote reçu dans la même session informatique que l'identification (bulletin qui est, par ailleurs, reçu en clair[5]). Elle n'est, de plus, pas la seule a avoir accès à cette identification[6].

➔ Dans le troisième système, l'entrée dans le processus de vote se fait nominalement (guichet unique) et il n'y a ensuite pas de réelle scission avec la traçabilité du bulletin de vote.

➔ Dans deux de ces systèmes, seul le canal TSL/SSL protège le contenu du bulletin; donc, si le flux passe[7] par un serveur mandataire "proxy SSL" (ouvrant), la session, et par là le contenu du bulletin, sont connus et ce, à l'insu du votant.

2. Dans les deux de ces systèmes, où seul le canal TSL/SSL protège le contenu du bulletin, l'attaque par "écoute" du calcul impliquant la clef privée (du serveur) suffirait pour connaître le contenu des bulletins (Jean-Pierre Seifert, Timing Attack Against RSA) [cas repris plus bas].

- Le dépôt du bulletin de vote rempli avec l'adresse IP du poste de l'électeur permet, grâce aux bases de données d'accès public de géolocalisation[8], de savoir d'où le vote a eu lieu, voire -si l'administration a accès à l'opérateur du réseau expéditeur- de connaître le titulaire de l'adresse.
- Aucun de ces systèmes n'a de transparence démocratique, par absence de possibilité de scrutation intégrée au protocole (architecture pure client-serveur non effectivement auditable, dite black-box[9]);
- Il n'y a pas création de preuve que chaque citoyen a pu user de son droit de

---

l'urne électronique) pour traiter les contestations.
Dans cette architecture eVoting, l'administration publique est donc et dois être en mesure de relier un citoyen et un bulletin.
De plus, même si les bulletins étaient insérés anonymes* et dans un ordre non séquentiel dans l'urne (ODP art 27h al.2), il resterait l'existence des journaux (log) constitués par le serveur (et le firewall, et la base de données, etc.) permettant de retrouver le bulletin lié à la session du citoyen (son numéro). Ces journaux sont nécessaires pour la bonne gestion technique des systèmes, et comme éléments de preuve lors des contestations ou d'indices lors d'enquêtes de piratage.
(*) les bulletins ne devraient pas être dégarnis jusqu'au strict contenu, car ils doivent encore porter la preuve de leur authenticité et intégrité.

5 Dans la schéma de fonctionnement de deux des pilotes, le bulletin est envoyé en clair (non chiffrés) aux serveurs de l'administration pour permettre le réaffichage de contrôle avec les imagettes (ou l'image) contenant le filigrane de vérification du serveur.

6 La liste des couples < noms ↔ numéros de vote > est envoyée à l'imprimeur pour l'édition des cartes de vote.
Chez l'imprimeur, elle est copiée sur ses nombreux systèmes (p.ex. gestion administrative du travail, commande générale de l'atelier des machines d'impression, etc.). La liste transite dans son réseau local, passant par les ordinateurs d'infrastructure, avant d'alimenter les machines d'impression. Ces imprimantes industrielles sont pilotées chacune par un ordinateur, qui stocke l'information à imprimer.
Chez un tiers, la liste est donc répliquée en de multiples exemplaires, automatiquement par les systèmes intermédiaires, dont l'ensemble sera difficile -voire impossible- à complètement supprimer

7 Soit le navigateur a été configuré à cet effet pour l'accepter (p.ex. au sein d'une entreprise ou administration).
Soit le navigateur contient un certificat reconnaissant une racine de CA dont le proxy a la clef privée. Ce dernier s'interpose dans le flux https en générant lui-même un certificat authentifiant le site demandé par l'utilisateur, et déchiffrant au vol le trafic pour l'étudier, avant de le rechiffrer pour le véritable site cible. Ex : modèle Palo Alto Network PA-4000, cité in The Risk Digest Volume 25, issue 50 Fri, 2 Jan 2009

8 P.ex. (il y a plus précis) : http://www.ip2location.com/ : "identify visitor's geographical location ie. country, region, city, latitude, longitude, ZIP code, time zone, connection speed, ISP and domain name".

9 L'étude (audit) du texte source est insuffisante, car elle ne prouve rien sur le programme effectivement exécuté (changements ultérieurs, "patch" binaires, appels de logithèques externes, etc.).

vote, et ce de manière unique, exhaustive et exclusive.

- Il n'y pas la garantie que le bulletin soit intègre lors du dépouillement, (c-à-d. la preuve que chaque bulletin contient exactement la motivation du votant).
- Il n'y a pas possibilité de démontrer que l'urne contient tous les bulletins authentiques, et seulement eux (pas de preuve qu'il n'y a ni bulletins ôtés, ni ajoutés).

1. Au moins un ces systèmes présente des vulnérabilités excessives :
   - À la **multiplication du vote**, plusieurs bulletins sont générables lors d'une même session d'un votant et cette attaque est détectable. Étonnamment, le résultat est … rectifiable dans l'urne et le fraudeur sans autre identifiable (ce qui est anormal en regard du secret du vote et de l'anonymat du votant !).
   - À la **falsification[10] massive des votes**, ceci par attaque du MS-IExplorer avec un hook-virus (forme utilisée contre des banques US [B.Schneier] et démontrée par le LASEC/EPFL). Le virus modifie, totalement à l'insu du votant et sans laisser de traces, le contenu du bulletin. L'attaque démontrée est indétectable (aucune trace), le virus est furtif (il s'efface après l'opération), le résultat est non rectifiable, l'impact très large [Dr Ph.Oechslin/LASEC-EPFL].
   - Car sa détection du vol falsifiant de votes est inefficace. Les codes filigranes des imagettes identifiantes peuvent être décodés et donc recomposés; ils sont similaires aux techniques CAPTHA[11] très largement contournables[12].
   - Et est excessivement fragile lors de l'exploitation (saturation des structures, bourrage de la mémoire, etc.).

3. Au moins un de ces systèmes a une absolue pauvreté de définition des données : totale absence de contrainte de validité sur ses données élémentaires et une parfaite faiblesse de structuration de celles-ci (données complexes). L'état technologique est celui des années septante. Outre la difficulté de maintenance, il n'y a aucune détection intégrée de perte de fiabilité (falsification des prédicats d'exécution), ce qui empêche toute sécurité.

4. Au moins un de ces systèmes utilise la cryptographie de manière insuffisante ou erronée : la sécurité du bulletin repose uniquement sur la fonction de hachage SHA-1 qui a été attaquée avec succès et doit être remplacée par SHA-256 au moins, (B.Schneier et USA-NSA B'list): et il utilise pour chiffrer le bulletin un surchiffrement RSA, ce qui est erroné [cas repris plus bas].

5. Au moins deux de ces systèmes, si ce n'est les trois, sont potentiellement vulnérables à la falsification du site de vote. La sélection du site se faisant par le seul pointage du navigateur par le citoyen, la direction peut être erronée -par faute de frappe ou redirection frauduleuse (virus, attaque DNS)- et le certificat doit être

10 Un autre des trois systèmes a un fonctionnement quasi identique, bien que largement plus résistant à cette attaque (et plus résistant au contournement du filigrane), mais ce au prix d'une lourdeur de traitement et de transport.

11 Completely Automated Public Turing test to tell Computers and Humans Apart.

12 Exemples de décodeurs de CAPTCHA : http://sam.zoy.org/pwntcha/ (2007) ou http://www.brains-n-brawn.com/default.aspx?vDir=aicaptcha (2005) ou http://www.cs.sfu.ca/~mori/research/gimpy/ (2002)

scrupuleusement vérifié à chaque fois par le citoyen.

6. Pour les trois systèmes, le certificat du site de vote peut être vulnérable à une attaque par collision (dite des anniversaires). Les implantations de la norme X.509, employant usuellement un hachage faible MD5, il est possible de générer deux certificats de sujet identique, valablement et identiquement signés[13] par l'Autorité de Certification, mais pour deux clefs différentes (Arjen Lenstra, Colliding X.509 certificates for different identities). L'empreinte numérique (condensé, trace, hash code, fingerprint) étant la même pour les deux certificats, le votant ne peut donc pas voir la différence.

7. Pour les trois systèmes, la clef du site de vote peut avoir été menacée sans qu'il soit possible de contrer efficacement l'attaque. Les navigateur (browsers) courants tels MS-Internet Explorer ou Mozilla Firefox ne contrôlent pas l'état de révocation du certificat par défaut; le certificat d'une clef atteinte (et donc révoquée) sera donc utilisé et accepté.

8. Dans les deux de ces systèmes, une seule attaque peut ruiner l'ensemble. Dans ces deux systèmes, où seul le canal TSL/SSL protège l'ensemble des transactions (dont le bulletin), un logiciel malveillant injecté dans le serveur (frontal) de ces systèmes permet, au moyen de l'attaque par "écoute de tempo" du calcul impliquant la clef privée (du serveur), de connaître celle-ci (J-Pierre Seifert, Timing Attack Against RSA[14]).

9. Les capacités (débit) de ces systèmes sont trop faibles. Pour l'un, le maximum de sessions simultanées est très limité -25-, alors que l'ensemble de l'opération de vote d'un citoyen représente une seule session (virtuelle) et donc bloque longuement cette ressource. Les données manipulées sont inutilement et excessivement grosses, et les outils logiciels d'exploitation trop limités, ce qui cause des blocages après une ou deux dizaines de milliers de votes, ou nécessite une réinitialisation quotidienne.

10. Au moins un de ces systèmes ne fait pas de sauvegarde distante (la seule tolérance aux pannes est que les disques sont localement dupliqués -RAID 1-). Si l'armoire du serveur brûle, les votes sont intégralement perdus.

11. Aucun de ces systèmes n'a de prouvabilité cryptographique (ou mathématique) de bonne fin, et aucun ne permet la résolution des contestations (réclamation avant clôture, ou plainte durant la période de recours).

12. Aucun de ces systèmes n'est basé sur le principe universel d'identité numérique, outil parfait de sécurité informatique et de protection juridique. Inversément, en dotant (par l'usage même) la population d'une telle identité, il est possible d'obtenir un gain économique, un meilleur service et une très forte diminution des coûts.

13. Utilisation d'outils de développement ou d'exploitation faible :

13 Un seul certificat est signé, mais la signature de l'Autorité de Certification est valable pour les deux (certificats ou clefs). Si les numéros de certificats sont en tête et imprévisibles, l'attaque n'est plus possible. Il n'est -actuellement- pas non plus possible de générer un second certificat valide après coup (attaque sur la seconde préimage).

[bis] Une amélioration de l'attaque, par trois centres de recherche (CWI, EPFL, TU/e), permet de générer un certificat de contenu quelconque et validement authentifié (indirectement) par une autorité (EPFL, 30 déc. 2008). Voir aussi la discussion sur la sécurité effective http://www.schneier.com/blog/archives/2008/12/forging_ssl_cer.html

14 L'attaque est actuellement ciblée sur la bibliothèque OpenSSL et les processeurs Intel usuels.

- tel le langage Java au parallélisme non sûr (P.B.Hansen), à l'environnement d'exécution (JVM -Java Virtual Machine) vulnérable (B.Schneier) ou aux classes (bibliothèque standard) aisément corruptibles par piratage (LASEC/EPFL). Mauvaise gestion de la mémoire.
  Il est à noter que C et C++ sont aussi déconseillés pour l'écriture de logiciels sécurisés (B.Schneier).
- ou l'utilisation exclusive pour voter d'un navigateur (browser, sp. MS-InternetExplorer) permettant l'extension par des ancrages logiciels (hook) et très vulnérable à une attaque virale pouvant être aisément massive sur la population (P.Öchslin/LASEC-EPFL).

14. Mise en oeuvre de méthodes[15] cryptographiques faibles, obsolètes, erronées ou percées (attaquées) : RC/4 (affaibli, exclu de NESSIE[16]), les clefs symétriques sont trop courtes, (conseillé 196 ou standard 256, NESSIE), SHA-1 (attaqué avec succès[17], doit être remplacé par SHA-256 au moins, B.Schneier et USA-NSA B'list), clefs asymétriques RSA-1024 (trop faibles[18], devrait être actuellement de 3072 et augmenté, NSA/NIST-elliptic), etc.

15. Dans un de ces systèmes, le chiffrement (terminal) du bulletin est mal effectué : deux clefs sont utilisées consécutivement; or, un surchiffrement RSA est erroné, car l'algorithme est un groupe (math.) et cela est équivalent à un chiffrement simple sous une clef tierce, avec en plus le risque de créer une clef résultante faible.

16. Envoi du bulletin par SMS, non secret (pour l'administration), utilisant des codes incompréhensibles, ne permettant pas la quittance de bonne fin, lié par la norme technologique à l'expéditeur (via l'opérateur), ou encore extrêmement vulnérable à une attaque en déni de service (B.Schneier http://www.smsanalysis.org/).

17. Manque d'ergonomie :

- l'un de ces systèmes oblige le citoyen à passer préalablement à la mairie pour signer un contrat d'utilisateur individuel, et de recevoir, gérer et conserver une grille de codes à biffer.
- Un autre système oblige le citoyen à employer, pour exprimer son vote, des codes complexes illisibles (SMS).
- Deux de ces systèmes obligent le citoyen à contrôler la bonne fin en comparant des codes cryptiques entre sa carte de vote et l'écran.
- Les systèmes exigent que le citoyen vérifie à chaque vote la très longue trace numérique du certificat (SSL) du serveur par comparaison avec la carte de vote.

15 La plupart de ces incorrections ne sont pas "tragiques" aujourd'hui -en partie car la durée du secret est courte-, mais désagréables pour le sérieux de ces projets et inadéquates pour un usage futur.

16 NESSIE New European Schemes for Signatures, Integrity and Encryption, est le résultat d'un projet européen (UE) mené de 2000 à 2003 pour identifier les moyens (algorithmes) cryptographiques sûres.

17 Aussi 16 juin 2009 « A new attack [...] find collisions in 2^{52} hash operations -- well within the realm of computational possibility. Assuming the cryptanalysis is correct, we should expect to see an actual SHA-1 collision within the year » & « remember the great truism of cryptanalysis: attacks always get better, they never get worse. » http://www.schneier.com/blog/archives/2009/06/ever_better_cry.html

18 Une clef de 1023 bits (non "semi-première"/choisie) a été factorisée avec succès par l'EPFL en mars 2007 (A.Lenstra). Un nombre mathématiquement spécial, or la technique sera tôt ou tard généralisée aux nombres RSA.

- Aucun des systèmes ne permet l'interruption et la reprise de la procédure de vote - et en cas de panne, l'opération est perdue !

18. Deux de ces systèmes ont un coût élevé d'opération à cause de l'emploi de carte de vote avec un champ secret sous une gomme métallique à impression holographique, ou une couche semi-transparente avec couverture à détacher. Le troisième système nécessite la gestion par l'État des validités et des envois de grilles de codes à biffer.

19. Deux de ces systèmes ouvrent la voie à la vente de vote en permettant une certaine preuve de vote par fourniture d'un récépissé imprimable[19] contenant les choix du bulletin ainsi qu'une authentification personnalisée du votant.

20. Un de ces systèmes utilise un système de protection de code secret (Hydalam™) qui est vulnérable (Cambridge University).

Pour résumer l'essentiel, un système de vote par internet devrait répondre obligatoirement à ces grands critères :

- **assurer la sécurité (résistance aux attaques informatiques) et ce intrinsèquement,**
- **garantir inconditionnellement l'anonymat du votant et le secret du vote,**
- **respecter la temporalité du vote (bulletins clos jusqu'au dépouillement),**
- **permettre la transparence de l'opération (scrutateurs) et la prouvabilité de bonne fin et des résultats,**
- **assurer une et une seule voix pour chaque citoyen et ce exclusivement,**
- **maintenir la preuve de la motivation du votant, de son expression jusqu'au dépouillement,**
- **ne pas permettre la vente de vote (pas de preuve du contenu du bulletin),**
- **être ergonomique,**
- **être économique (y compris offrir un débit confortable),**
- **être techniquement de qualité (architecture élégante, outils puissants, code fiable, définitions de données sémantiquement riches) pour permettre une exploitation et une maintenance optimales.**

Et cela n'est pas le cas pour les pilotes actuels.

La sécurité doit être intégrée en première ligne dans l'architecture conceptuelle du système, et non pas vouloir être ajoutée après coup. Il est peine perdue d'installer par la suite une grosse serrure sur la porte, ou des barreaux aux fenêtres, d'une cabane en bois; comme celle de la fable des trois petits cochons...

19 La suppression de la capacité d'impression du navigateur peut être inhibée par des options de celui-ci.