La solution genevoise de vote électronique à cœur ouvert

Michel.Chevallier@etat.ge.ch, Chancellerie d'Etat de Genève, Responsable de la communication du vote en ligne & Agatha Bahègne-Bradley, Christophe Vigouroux, François Montmasson, Rémi Villemin et Franck Ponchel, du Centre des Technologies de l'Information de l'Etat de Genève

This article offers an unprecedented glimpse into the functioning and architecture of the Geneva internet voting system, one of the most advanced in the world.

Cet article lève le voile sur le fonctionnement et l'architecture du système genevois de vote par Internet, l'un des plus performants à l'heure actuelle

Le système suisse de démocratie dite *semi-directe* permet aux citoyens de se prononcer sur toute loi adoptée par n'importe quelle autorité (communale, cantonale ou fédérale) et de proposer de nouvelles lois, pour autant qu'ils réunissent le nombre de signatures requis. Ainsi, les Helvètes sont-ils appelés aux urnes quatre à six fois par an pour confirmer ou rejeter les décisions de leurs élus. En conséquence, l'accessibilité aux scrutins, de même qu'une bonne organisation électorale, sont essentielles à l'exercice harmonieux des droits démocratiques en Suisse.

Dans ce contexte, le vote postal s'est développé jusqu'à être utilisé, selon les cantons, par deux tiers à 95% des votants. Il y a plus: en facilitant l'accès au vote, le vote postal a par exemple permis à Genève d'augmenter la participation moyenne de 20 points. Ce succès, ainsi que le constat que le vote postal ne résout pas le problème d'accessibilité des électeurs de l'étranger et des personnes à mobilité réduite ou malvoyantes, a ouvert la voie au vote par Internet. Il existe aujourd'hui à Genève trois canaux de vote parfaitement intégrés: les locaux de vote, la voie postale et Internet.

Le premier vote électronique de Suisse a eu lieu en janvier 2003 à Genève. À ce jour, 19 votations et trois élections à caractère administratif mettant en jeu le vote électronique ont eu lieu dans ce canton. Aucune autre collectivité publique au monde n'a une telle expérience en matière de vote en ligne.

Le vote par Internet amène des enjeux supplémentaires par rapport au vote postal, en raison de la dématérialisation des suffrages. Comment se déroule une opération de vote ? Quelles sont les mesures de sécurité mises en œuvre ? Comment garantit-on le secret du vote ? Autant de questions auxquelles cet article a pour but d'apporter des éléments de réponse. Il s'adresse à un public technique ayant des connaissances de base en cryptographie. Dans les pages qui suivent, nous utiliserons indifféremment les expressions *vote électronique*, *vote en ligne*, *eVoting* et *vote par Internet* pour parler du vote par Internet pratiqué à Genève.

Les aspects abordés dans cet article sont structurés selon les quatre étapes principales du cycle de vie d'un scrutin incluant le vote électronique (fig. 1).

Initialisation d'une opération

Durant la phase d'initialisation, les données nécessaires à l'opération électorale sont importées dans le système eVoting. Ces données proviennent de plusieurs sources et sont de natures différentes. On distingue en particulier:

- Les données de rattachement électoral: communes et locaux de vote, en particulier les communes autorisées à voter par Internet pour l'opération concernée lorsque le plafond prévu par l'ordonnance fédérale sur les droits politiques s'applique.
- Les données relatives aux objets de vote: sujets de vote (votation) ou listes de candidats (élection).
- Les données de rattachement géographique: liste de pays (pour les Suisses de l'étranger en particulier), liste des cantons, etc.
- Les données nécessaires à la production du matériel de vote: registre électoral avec nom, prénom, adresse, notamment.
- Les données nécessaires à l'authentification des électeurs sur le système de vote électronique: date de naissance, commune d'origine.

Les données nominatives provenant du registre des habitants de l'Office cantonal de la population et permettant de produire les fichiers à destination des imprimeurs ne sont pas conservées en base de données.

Les fichiers imprimeurs contiennent également les données de vote (numéro de carte de vote, mot de passe et code de contrôle) qui ont été générées à l'aide d'un générateur quantique d'aléas. Ces données sont spécifiques à chaque électeur et à chaque opération.

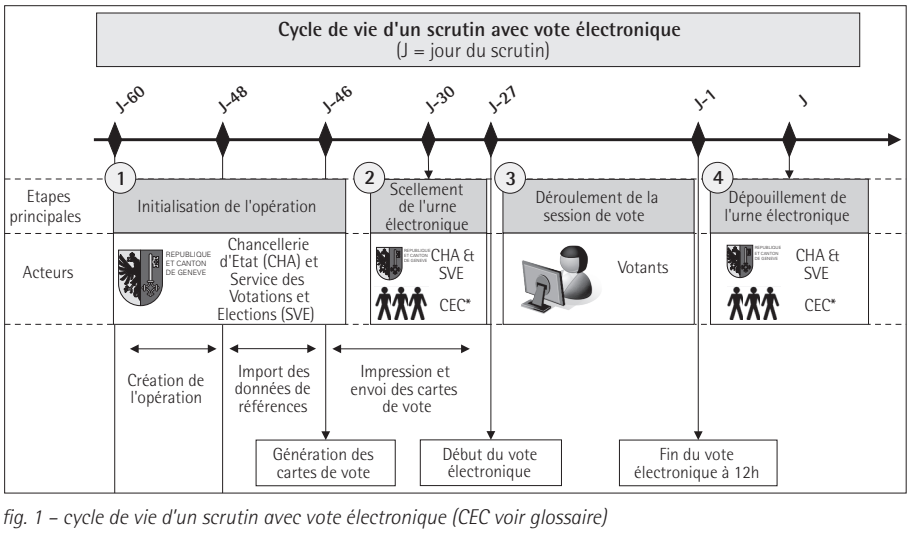

fig. 1 – cycle de vie d'un scrutin avec vote électronique (CEC voir glossaire)

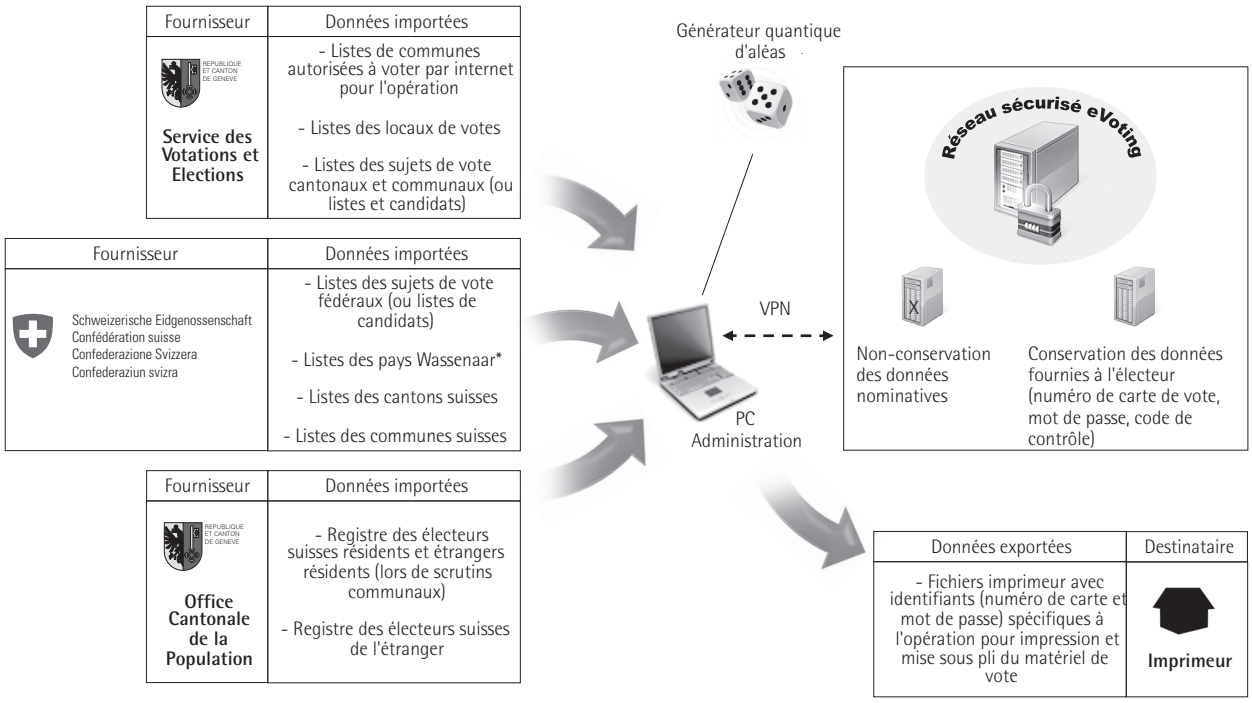

fig. 2 – flux de données lors de la phase d'initialisation d'une opération (pour la liste des pays Wassenaar, voir le glossaire)

Les flux de données lors de la phase d'initialisation peuvent être représentés de la manière suivante (fig. 2).

Scellement de l'urne électronique

Le scellement de l'urne électronique a lieu lors d'une séance officielle de préparation de la session électorale et de génération des clés de chiffrement des votes. L'étape s'effectue alors que les informations reproduites sur les cartes de votes ont été importées dans le système et que les cartes ont été imprimées et sont en cours d'envoi.

Lors de cette étape, des moyens cryptographiques sont mis en place afin de garantir l'inviolabilité de l'urne. Une urne est inviolable si on ne peut ni y écrire ni y lire des votes à l'insu du système.

- L'urne est illisible pendant la session de vote grâce à l'utilisation d'une clé asymétrique où seule la clé publique de chiffrement est disponible et la clé privée de déchiffrement mise en lieu sûr et protégée par des mots de passe.
- L'urne est inaltérable à l'insu du système grâce à l'utilisation de la clé publique de chiffrement des votes et d'un compteur d'intégrité connus seulement par le système de vote.

La clé publique de chiffrement est connue seulement par le système et est la seule capable de déposer des votes valides dans l'urne. Un vote valide est un vote correctement décryptable par la clé privée.

Le compteur d'intégrité indique le nombre de votes présents dans l'urne. Afin de résister à un redémarrage du système et d'être inaltérable, ce compteur est stocké encrypté avec une clé symétrique dans la base de données.

Préparation de l'étape

Les différents acteurs ainsi que le matériel nécessaires au scellement de l'urne électronique sont réunis. L'étape se déroule selon un protocole établi par la Chancellerie.

Les acteurs de cette étape sont:

- la Chancelière d'État ou le Vice-Chancelier,
- le Président de la CEC,
- le Président de Séance,
- deux groupes d'au moins deux membres de la CEC,
- le représentant du Service des Votations et Élections,
- un notaire,
- l'officier de sécurité des systèmes d'information de la Police (ci-après *officier de sécurité*),
- l'administrateur eVoting.

L'administrateur eVoting se connecte de façon nominative au système de vote électronique avec le PC d'administration dédié, à travers un VPN sécurisé à secret unique sur une prise réseau dédiée.

L'administrateur eVoting lance la console d'administration. Cette application fournit une interface graphique qui encadre le déroulement de chaque étape.

Génération des clés

Clés	Utilisation
Clé publique de chiffrement des votes	Cette clé permet de chiffrer les votes dans l'urne, mais ne permet pas de les déchiffrer.
Clé privée de déchiffrement des votes	Cette clé permet de déchiffrer les votes dans l'urne et d'obtenir le résultat du scrutin.
Clé symétrique du compteur d'intégrité	Cette clé permet de chiffrer et de déchiffrer le compteur d'intégrité dans la base de données et d'assurer l'inaltérabilité de l'urne.

tableau 1 – clés du système produites pendant l'étape de scellement de l'urne

L'administrateur eVoting lance la génération:

- de la paire de clés asymétriques de chiffrement des votes qui se compose
  - d'une clé publique de chiffrement des votes,
  - d'une clé privée de déchiffrement des votes;
- de la clé symétrique du compteur d'intégrité.

Afin de protéger l'accès à la clé privée de déchiffrement des votes, celle-ci est stockée dans un trousseau de clés protégé par 2 mots de passe.

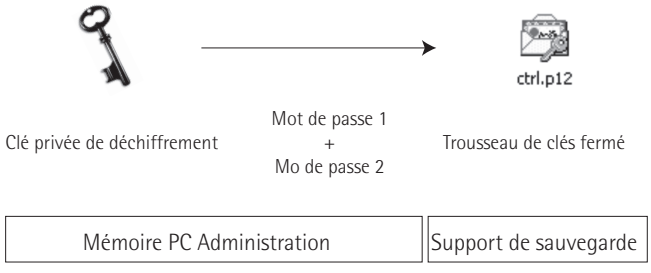

fig. 3 – trousseau de clés protégé par 2 mots de passe

Chacun des deux groupes de membres de la CEC choisit un mot de passe et le saisit sur un formulaire *ad hoc*. La première personne du premier groupe saisit le mot de passe choisi par son groupe. La seconde personne saisit le même mot de passe afin de confirmer la saisie. La même procédure est effectuée par le second groupe pour le second mot de passe.

Stockage

Trois ensembles de données sont directement générés sur 2 supports amovibles (une clé USB et un CD) afin de ne pas être sauvés sur le PC Administration:

- le trousseau de clés protégé par mots de passe,
- la clé publique de chiffrement des votes,
- la clé symétrique du compteur d'intégrité.

L'administrateur eVoting transfère une copie de la clé symétrique du compteur d'intégrité sur le système. Ces supports sont mis sous enveloppes scellées puis remis à l'officier de sécurité. Les formulaires de saisie des mots de passe sont mis sous deux enveloppes distinctes, scellées puis remises au notaire.

Enfin, l'administrateur eVoting lance l'initialisation finale de la base de données eVoting en affectant le compteur d'intégrité à 0 avec la clé symétrique.

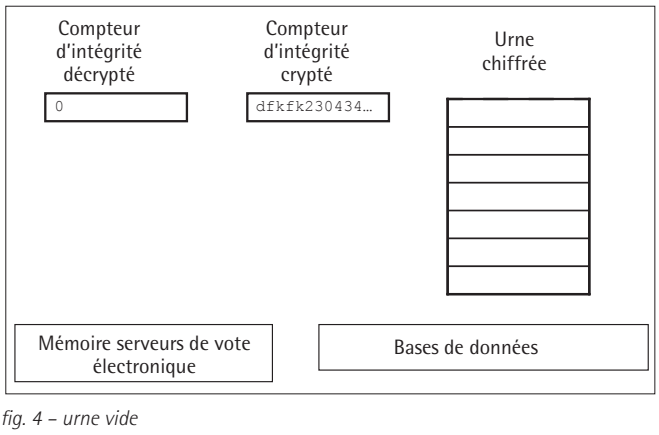

fig. 4 – urne vide

Secret	Créateur	Support de sauvegarde
Mot de passe 1	Premier groupe de membres de la CEC	Formulaire de saisie 1
Mot de passe 2	Second groupe de membres de la CEC	Formulaire de saisie 2
Trousseau de clés protégé par mot de passe	PC Administration	CD et clé USB
Clé publique de chiffrement des votes		CD et clé USB
		Disques durs du système de vote électronique
Clé symétrique du compteur d'intégrité		CD et clé USB
		Disques durs du système de vote électronique

tableau 2 – liste des secrets

À noter qu'aucun des secrets ne reste sur le PC d'administration. Un vote de test est alors effectué sur le système par chacun des groupes. Les résultats attendus sont notés.

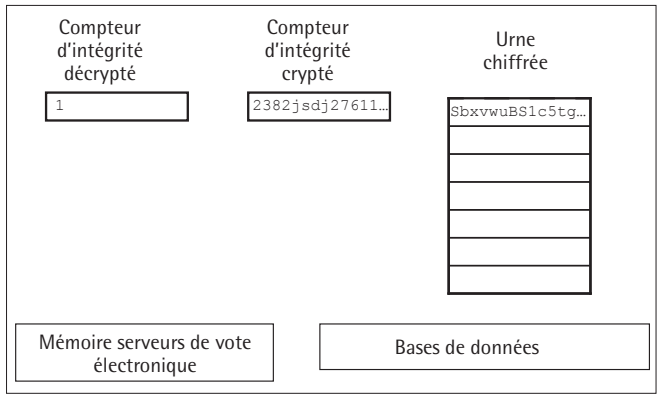

fig. 5 – premier vote de test dans l'urne

Le dépouillement de l'urne est effectué (voir explications ci-après) et les résultats obtenus sont validés.

Le PC Administration est mis dans un sac qui est ensuite scellé par des plombs numérotés, dont les numéros sont relevés. Le sac est remis au représentant du Service des Votations et Élections qui le conservera pour la durée du scrutin.

Support de sauvegarde	Support d'intégrité	Propriétaire pendant la session de vote
PC Administration	Sac plombé	Représentant du service des votations
Formulaire de saisie 1	Enveloppe scellée 1	Notaire
Formulaire de saisie 2	Enveloppe scellée 2	
CD et Clé USB	Enveloppe scellée 3	Officier de sécurité

tableau 3 – liste des supports de sauvegarde

Les flux de données lors du scellement de l'urne peuvent être synthétisés comme le montre la figure 6.

Comment être sûr que l'urne ne pourra pas être ouverte avant l'étape de dépouillement de l'urne ?

Afin d'ouvrir l'urne, il faut réunir des secrets en possession d'acteurs différents sur des supports protégés. Chaque acteur n'a au plus qu'un secret en main. Pour introduire ces secrets dans le système et déverrouiller l'urne, il faut se connecter à une infrastructure sécurisée. Aucun acteur en possession d'un secret n'a accès à cette infrastructure.

Comment être sûr de pouvoir réunir les secrets afin d'ouvrir l'urne ?

Chacun des secrets est disponible sur deux supports:

Secrets du scrutin	Support de sauvegarde
Mot de passe 1	1. Enveloppes contenant les mots de passe chez le notaire 2. Mémoire des personnes du groupe 1 de membres de la CEC
Mot de passe 2	1. Enveloppes contenant les mots de passe chez le notaire 2. Mémoire des personnes du groupe 2 de membres de la CEC
Trousseau de clés protégé par mots de passe	1. CD chez l'officier de sécurité 2. Clé USB chez l'officier de sécurité des systèmes d'information
Clé publique de chiffrement des votes	1. CD et Clé USB chez l'Officier de sécurité 2. Disques durs du système de vote électronique
Clé symétrique du compteur d'intégrité	1. CD et Clé USB chez l'Officier de sécurité 2. Disques durs du système de vote électronique

tableau 4 – Redondance des secrets sur les supports

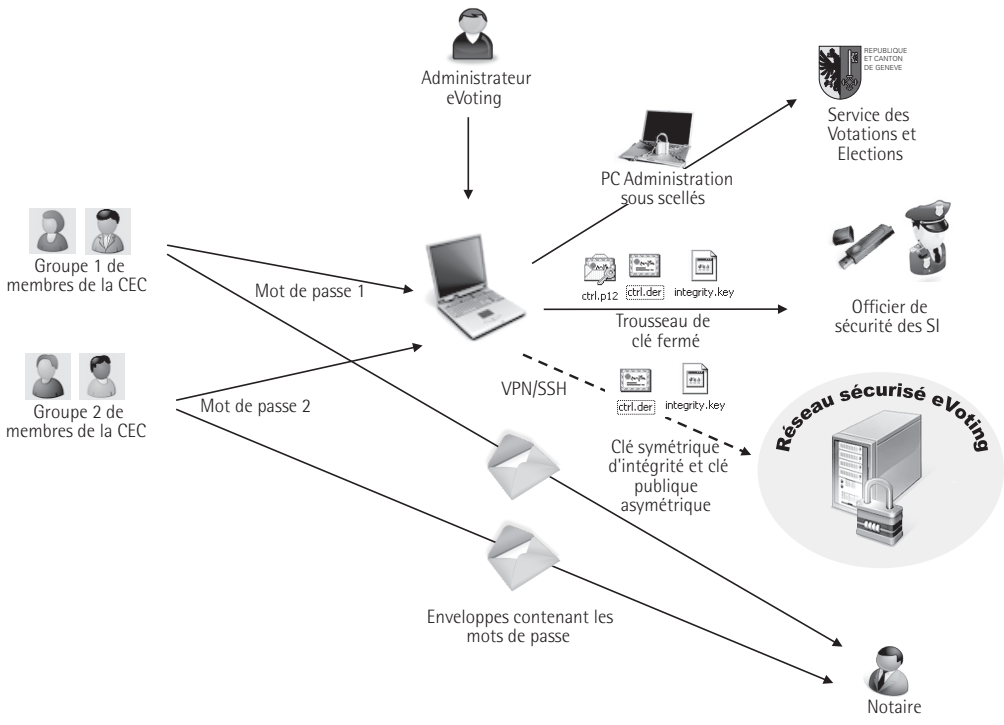

fig. 6 – échange des secrets et des supports de sauvegarde

Déroulement de la session de vote

Une fois l'urne électronique scellée, le site de vote par Internet peut être ouvert au public.
Lorsqu'un électeur se connecte sur **https://www.evote-ch.ch** avec son navigateur Web, il démarre une session de vote.
Pour mener à bien une session de vote, l'électeur commence par saisir son numéro de carte de vote sur la page d'identification, puis il accepte les avertissements légaux, saisit son bulletin de vote, vérifie son vote et fournit ses informations personnelles (mot de passe, date de naissance et commune d'origine) sur la page d'authentification, avant d'aboutir à la page de confirmation l'assurant de l'enregistrement de son vote.

Secret du vote	Origine	Support de sauvegarde
Date de naissance	Données personnelles de l'électeur	Registre des habitants Base de données Mémoire du votant
Commune d'origine		Registre des habitants Base de données Mémoire du votant
Mot de passe	Système de vote électronique	Base de données (haché) Carte de vote
Numéro de carte de vote		Base de données Carte de vote
Code de contrôle		Base de données Carte de vote

tableau 5 – secrets du vote

Une session de vote nécessite d'établir un dialogue entre le navigateur de l'électeur et les serveurs du système eVoting. Plusieurs questions se posent quant à la sécurisation de ces échanges:

- comment s'assurer que l'électeur s'adresse bien aux serveurs eVoting ?
- comment identifier l'électeur ?
- comment s'assurer qu'un tiers malveillant ne puisse ni intercepter ni manipuler les données échangées ?

Authentification du site eVoting

Lorsque le navigateur de l'électeur entre en contact avec le site de vote eVoting, l'utilisation du protocole https entraîne la mise en place d'une communication SSL. Lors de l'établissement de la communication, le navigateur demande au site eVoting de présenter son certificat électronique. Il s'agit d'une carte d'identité numérique délivrée par une autorité de certifica-

tion dont le rôle est d'assurer le lien entre une identité physique et une identité numérique.
En vérifiant le certificat reçu, le navigateur valide l'identité du site eVoting. Une fois la communication SSL en place, l'électeur a la garantie de s'adresser au véritable site eVoting, d'une part, et que tous les échanges entre le navigateur et les serveurs eVoting sont chiffrés, d'autre part.

Identification de l'électeur

Pour chaque opération de vote, l'électeur reçoit par la poste une carte de vote à usage unique. À chaque électeur correspond en outre un numéro de carte de vote unique (NCV), permettant de l'identifier auprès du système de gestion des scrutins, quel que soit le canal qu'il choisira pour exprimer son suffrage.
Afin de ne pas compromettre cette information cruciale, celle-ci n'est jamais échangée. À la place, c'est l'empreinte du numéro de carte de vote qui est envoyée. Cette empreinte est obtenue en appliquant une fonction de hachage cryptographique ($Hash_E$) au numéro de carte de vote, ce qui rend très difficile, voire impossible dans les délais de l'opération de vote, de retrouver le numéro original. Le système eVoting utilise une table de correspondance, établie lors de l'étape de génération des fichiers imprimeurs, pour déterminer le numéro de carte de vote de l'électeur à partir de l'empreinte reçue. Dorénavant, le numéro de carte de vote constitue un secret dit *partagé* entre l'électeur et le système eVoting.

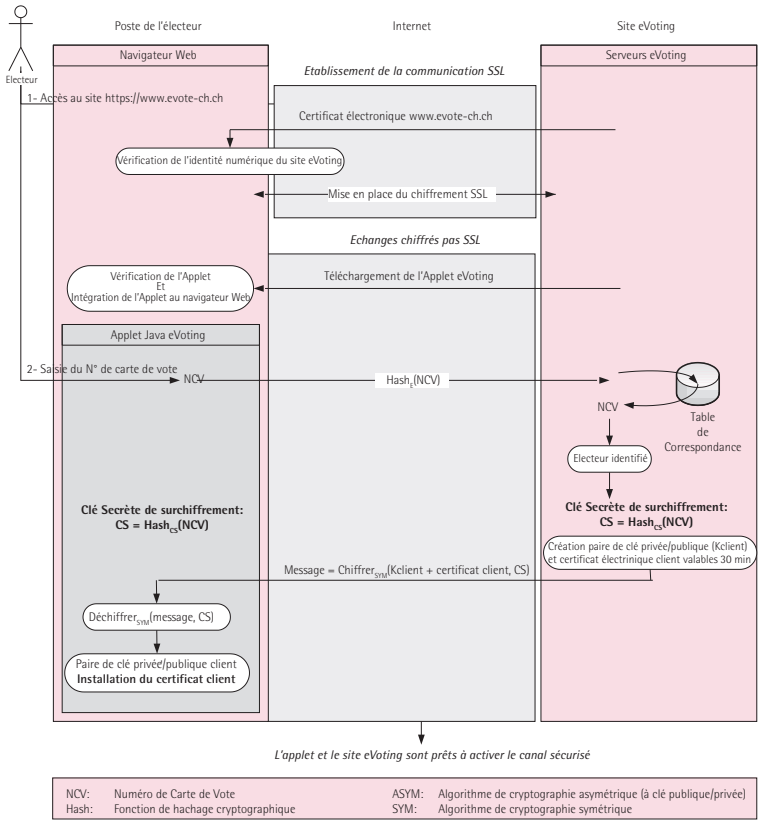

fig. 7 –phase d'authentification du site eVoting et d'identification de l'électeur

Canal sécurisé

Jusqu'ici, nous avons vu les mesures mises en place pour assurer à l'électeur qu'il s'adresse bien au site eVoting et comment le système eVoting identifie l'électeur. Nous allons aborder la manière dont les échanges sont sécurisés contre l'interception et la manipulation.

En effet, bien que le protocole SSL mette en place un chiffrement des échanges ainsi qu'une authentification du serveur, il a été prouvé que ce protocole est sensible aux attaques de type *man in the middle*. Bien que très complexe à mettre en œuvre, cette attaque consiste, schématiquement, à se placer entre le navigateur et le site eVoting. L'attaquant se fait alors passer pour le serveur eVoting auprès de l'électeur, et inversement, se fait passer pour l'électeur auprès du serveur eVoting.
Pour rendre ces attaques plus difficiles, le système eVoting met en place le concept de canal sécurisé entre le navigateur et le serveur. Le canal sécurisé s'appuie sur une combinaison de techniques de sécurité: protocole SSL mutuel, surchiffrement des données et authentification des messages.
Comme abordé plus tôt, le SSL *simple* requiert du serveur qu'il présente un certificat électronique au client afin que celui-ci puisse l'authentifier. Le SSL mutuel est une extension du SSL *simple* qui ajoute une phase d'authentification du client auprès du serveur. De la même façon, le client doit présenter son certificat électronique au serveur, qui le valide via une autorité de certification.
Une fois l'authentification mutuelle réalisée, le client est assuré de s'adresser au véritable site eVoting et le serveur est assuré de s'adresser à l'électeur. Dès qu'il est en place, le SSL mutuel assure un premier niveau de chiffrement de toutes les données échangées.
Le surchiffrement consiste à chiffrer les données au niveau de l'application, avant même de les envoyer via la communication SSL mutuelle. Le chiffrement s'appuie sur un algorithme de cryptographie à clé symétrique ($_{SYM}$), dont la clé secrète est dérivée du numéro de carte de vote (NCV), à la fois par le serveur et par le client, par utilisation d'une fonction de hachage cryptographique ($Hash_{CS}$). Les données sont donc chiffrées deux fois, de manière différente, lors de leur transmission, ce qui renforce la sécurité du chiffrement.
L'authentification des messages consiste à ajouter une empreinte chiffrée à chaque message. Concrètement, il s'agit pour le client de calculer l'empreinte du message (E_{MSG}), puis de chiffrer cette empreinte à l'aide de la clé privée associée à son certificat électronique (EC_{MSG}). Le chiffrage utilisé ici repose donc sur un algorithme cryptographique à clé asymétrique ($_{ASYM}$).
À réception du message chiffré et de son empreinte chiffrée, le système eVoting utilise la clé publique du certificat client pour déchiffrer la signature et obtenir l'empreinte du message (E_{MSG} reçue). Ensuite, le système eVoting calcule à son tour l'empreinte du message (E_{MSG} calculée). Si les deux empreintes diffèrent, c'est soit que le message original a été altéré, soit que le message n'a pas été signé par la clé privée associée à la clé publique du certificat client, donc pas par le client attendu !
Si les empreintes concordent, le système eVoting déchiffre le message à l'aide de la clé secrète et procède au traitement du message.
Les navigateurs Web actuels n'offrent pas les fonctionnalités suffisantes pour mettre en œuvre un canal sécurisé tel que nous venons de le décrire. Pour cette raison, le système eVoting requiert l'utilisation de la technologie Java, qui vient s'intégrer au navigateur Web de l'électeur pour l'enrichir.

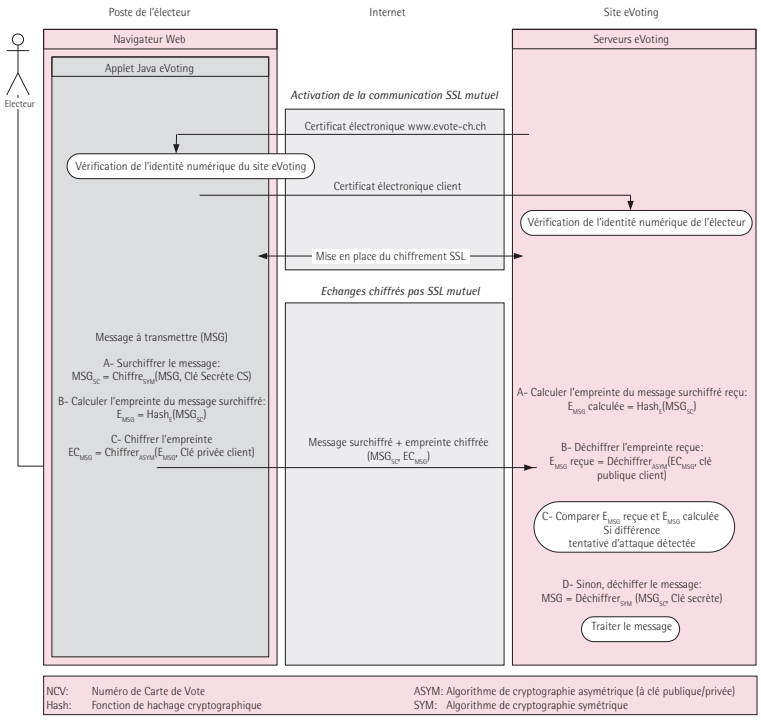

fig. 8 – établissement et utilisation du canal sécurisé

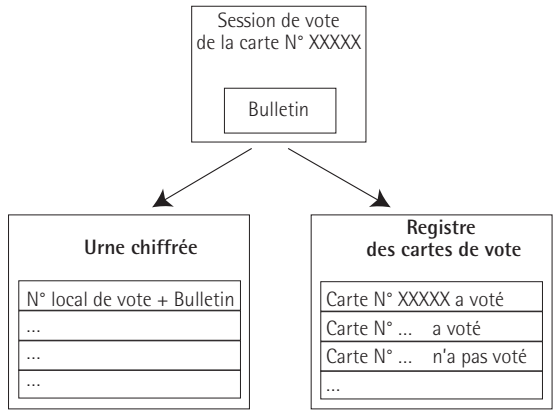

fig. 9 – séparation des données lors de l'enregistrement du vote

En pratique, dès le début de la session de vote, une applet Java est téléchargée depuis le site eVoting et exécutée au sein du navigateur Web sur le poste de l'électeur. Une fois le numéro de carte de vote saisi sur la page d'identification, l'applet met en place le canal sécurisé. L'applet et le navigateur Web s'intègrent de manière poussée afin que tous les échanges de données sensibles transitent par l'applet et non plus par le navigateur.

Enregistrement d'un vote dans l'urne

L'enregistrement d'un vote commence par l'indication par l'électeur de ses choix sur son navigateur. Le bulletin ainsi rempli est envoyé, via le canal sécurisé, au serveur de vote.

Le serveur déchiffre le bulletin de l'électeur, effectue un contrôle syntaxique (pour s'assurer que le vote exprimé sera valable afin d'éviter les nuls par erreur) puis renvoie à l'électeur une confirmation de ses choix avec un code de contrôle. Ce code aléatoire est inscrit sur la carte de vote de l'électeur et n'est connu que de lui-même et des serveurs eVoting: c'est une preuve supplémentaire pour l'électeur qu'il s'est bien connecté au serveur eVoting.

L'électeur est alors invité à s'authentifier en saisissant sa date de naissance, sa commune d'origine et le mot de passe inscrit sur sa carte de vote. Comme toutes données sensibles, celles-ci sont envoyées par le canal sécurisé au serveur de vote.

Le serveur vérifie les données personnelles de l'électeur, vérifie que l'électeur a le droit de voter (pas de vote préalable ni de vote par un autre canal), puis enregistre son vote (fig. 9).

- Le bulletin et le local de vote de l'électeur sont chiffrés avec du sel, en utilisant la clé publique de chiffrement de l'urne, puis enregistrés dans l'urne.
- Lorsqu'un citoyen vote, le registre des cartes de vote est modifié pour enregistrer le fait que le numéro de carte de vote associé à ce citoyen a voté.
- Le compteur d'intégrité lu en base de données est déchiffré par le système en utilisant la clé symétrique d'intégrité. L'application incrémente ce compteur, le chiffre à nouveau et le sauve en base de données.
- Ces trois opérations sont effectuées dans une même transaction de base de données afin de garantir que le dépôt du vote répond aux caractéristiques ACID (Atomicité, Cohérence, Isolation et Durabilité).

Finalement le serveur envoie à l'électeur une confirmation de son vote comprenant la date et l'heure de son vote, ainsi que le code de contrôle qui atteste que le message vient bien du système de vote.

Dépouillement de l'urne électronique

Le dépouillement de l'urne électronique a lieu lors d'une séance officielle. L'objectif de cette étape est d'extraire de l'urne électronique les résultats du vote.

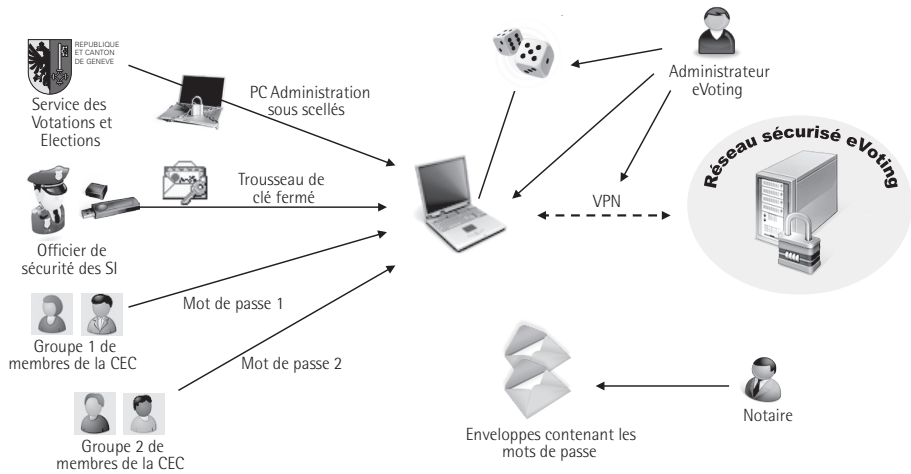

fig. 10 – Acteurs et matériels nécessaires au dépouillement de l'urne électronique

Déroulement de l'étape

Les différents acteurs ainsi que le matériel nécessaires au déchiffrement de l'urne électronique sont réunis. L'étape se déroule selon un protocole établi par la Chancellerie (fig. 10).

- Le responsable du Service des Votations et Élections (SVE) apporte le PC d'Administration sous scellés. Ces derniers sont cassés et vérifiés sous le contrôle d'un membre de la commission électorale centrale (CEC).
- L'administrateur eVoting connecte le PC Administration au réseau sécurisé eVoting. La salle où se déroule l'étape est équipée d'une prise spécifique, et seul l'administrateur possède les droits nécessaires à l'établissement d'un VPN. À cette étape, le générateur quantique d'aléas, apporté par l'administrateur, est connecté au PC Administration.
- L'officier de sécurité apporte le trousseau de clés électroniques fermé contenant la clé privée de déchiffrement des votes (supports clé USB et CD-ROM).
- Chacun des deux groupes de contrôleurs fournit son mot de passe permettant d'ouvrir le trousseau de clés. Au cas où l'un des groupes ne se souvient plus du mot de passe qui avait été défini, celui-ci peut être récupéré en ouvrant l'enveloppe correspondante apportée par le notaire.
- L'étape est conduite et supervisée par la Chancellerie.

Une fois les trois secrets - trousseau de clés, mot de passe 1 et mot de passe 2 - insérés dans l'application d'administration, celle-ci ouvre le trousseau pour récupérer la clé privée de déchiffrement des votes puis procède au déchiffrement de l'urne électronique et à la génération des résultats. Les modalités techniques de cette étape sont précisées dans le chapitre suivant.

Techniques de brassage de l'urne électronique et de déchiffrement

Bien que le système ait été conçu afin qu'il n'y ait aucune relation en base de données entre le registre des électeurs et l'urne électronique, il pourrait néanmoins exister la possibilité de faire un lien temporel entre un électeur, dont on enregistre l'instant du dépôt du vote, et le vote chiffré, celui-ci étant stocké par ordre d'arrivée. Différentes mesures techniques et organisationnelles empêchent cela. L'une d'entre elles consiste à brasser l'urne: tout comme pour une urne réelle, le déchiffrement de l'urne est précédé par un brassage dont le schéma suivant expose les principes (fig. 11).

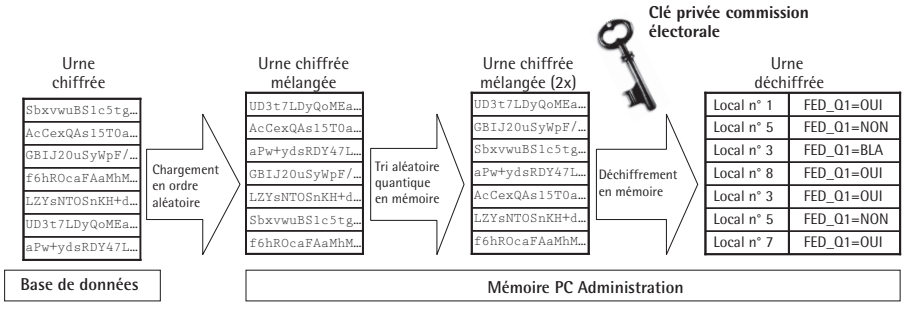

fig. 11 – brassage et déchiffrement de l'urne électronique

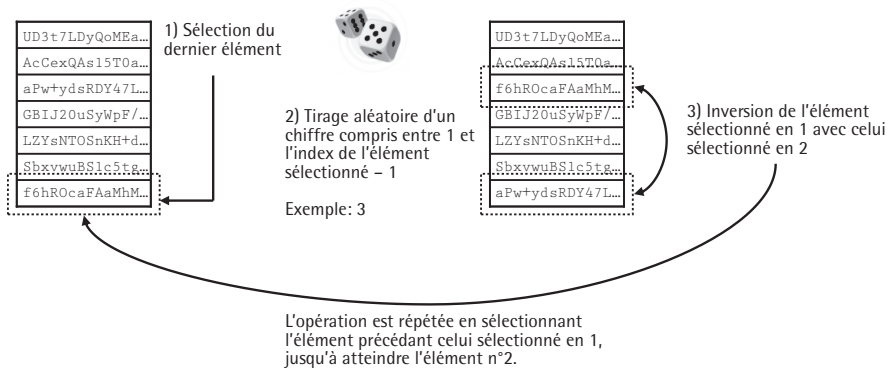

fig. 12 – algorithme du brassage quantique de l'urne

- Au départ, les votes chiffrés sont enregistrés en base de données dans leur ordre d'arrivée.
- La totalité des votes est chargée dans une structure en mémoire. Ce chargement utilise une fonctionnalité particulière de la base de données permettant de faire une lecture par ordre aléatoire.
- Cette première structure est à son tour mélangée en utilisant le générateur quantique d'aléas. Le schéma suivant expose le principe de ce mélange (fig. 12).
- Une fois l'urne mélangée deux fois, l'application ouvre le trousseau de clés en utilisant comme mot de passe la concaténation du mot de passe du groupe 1 puis du mot de passe du groupe 2 des contrôleurs de la CEC. La clé privée ainsi récupérée permet de déchiffrer chacun des votes et de constituer l'urne déchiffrée.

Le temps de déchiffrement unitaire d'un vote étant non négligeable, le choix a été fait d'exécuter en parallèle les processus de déchiffrement afin d'optimiser le temps de traitement de cette étape. Le schéma de la figure 13 expose ce principe.

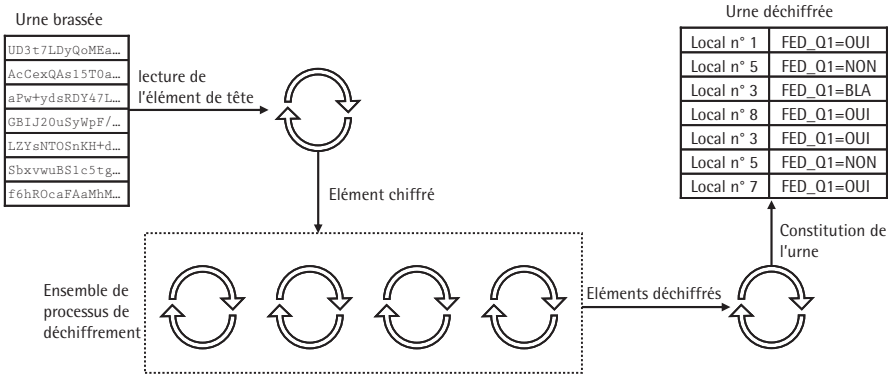

fig. 13 – traitement en parallèle du déchiffrement

- La structure représentant l'urne déchiffrée est utilisée par le traitement qui effectue les décomptes et génère les résultats du vote.

Comment être sûr que l'application comptabilise et enregistre les suffrages correctement ?

La CEC dispose d'un arrondissement électoral propre dans lequel elle émet des suffrages qu'elle protocole sur un formulaire papier. Les résultats de cet arrondissement sont vérifiés lors du dépouillement de l'urne électronique. Cela permet de vérifier que l'application n'introduit pas de biais dans les résultats.

Comment être sûr de prendre en compte tous les votes ?

Un compteur d'intégrité est incrémenté dans la même transaction que chaque vote enregistré dans l'urne chiffrée.
Lors du dépouillement de l'urne, une fonctionnalité de l'application d'administration permet aux différents acteurs de vérifier l'égalité de ce compteur avec le nombre de votes dépouillés et avec le nombre de votants ayant voté par Internet à partir du registre.

Comment être sûr qu'on ne peut pas faire de lien temporel entre l'électeur et son vote ?

Les 3 éléments suivants répondent à cette question:

- Le brassage quantique empêche de manière totale que l'ordre original des votes soit reconstitué en effectuant par exemple un brassage inverse.
- Le dépouillement s'effectue en mémoire sans journalisation.
- Les mêmes réponses n'ont pas la même valeur une fois chiffrée grâce à l'ajout d'un sel cryptographique différent pour chaque vote: on ne peut pas reconstituer l'urne chiffrée à partir de l'urne déchiffrée en analysant les résultats.

Conclusion

L'eVoting à Genève n'est pas un projet figé, mais s'inscrit au contraire dans un cycle d'améliorations continues. Les évolutions envisagées à long terme sont variées et innovantes: nouvelle certification ISO, sécurisation du poste du votant, accessibilité, etc.

Pour rester à la pointe des systèmes de vote par Internet et pour nous préparer aux normes dont l'OSCE et le Conseil de l'Europe débattent, nous travaillons également sur le thème de la vérifiabilité, afin de permettre à l'électeur de vérifier lui-même que son vote a correctement été pris en compte (norme dite *counted as cast* ou **compté tel qu'émis**) à l'image de la possibilité donnée aux citoyens d'assister au dépouillement dans les locaux de vote.
Dans le cadre de cet article, nous n'avons pu aborder l'ensemble des mesures prises pour garantir dans la mise en œuvre du vote électronique le respect de tous les principes qui président à la conduite d'un scrutin démocratique au sens des textes internationaux qui en donnent la définition. Il nous semble important de souligner en conclusion que le système de vote en ligne de l'État de Genève est parfaitement intégré au système général de gestion des scrutins, ne serait-ce que pour prévenir les votes multiples de citoyens facétieux.
En outre, l'État de Genève détient la propriété intellectuelle de son système, il en assure l'exploitation et les développements. Cette propriété est pour nous un élément essentiel de la légitimité du recours au vote électronique. Ainsi, tout ce qui vous a été présenté dans cet article appartient-il à l'État. Les diverses solutions évoquées ont souvent été développées spécifiquement pour être mises en œuvre dans l'application genevoise et sont sans équivalent ailleurs. ■

GLOSSAIRE

CEC: La commission électorale centrale (CEC) a été instituée au 1er janvier 2010, en même temps que le vote électronique était introduit dans la constitution cantonale genevoise. Selon la loi, la CEC ***a accès à toutes les opérations du processus électoral*** et peut ***procéder à des contrôles, en tout temps, indépendamment d'une opération électorale*** (article 75B de la loi sur l'exercice des droits politiques).
La CEC verrouille l'urne électronique en générant ses clés de chiffrement, de sorte que nul ne peut accéder aux suffrages électroniques avant le dépouillement. La CEC peut accéder à tout document relatif au système de vote électronique, elle peut mandater les experts de son choix pour des audits, des tests ou des études.
La CEC ainsi que les spécialistes qu'elle déciderait de mandater ont accès au code source en tout temps, de même que les personnes faisant état d'un intérêt académique.
Cette commission a créé en son sein un groupe technique qui a entamé un processus d'audit du système de vote électronique. La loi impose en outre que le système de vote par Internet soit audité tous les trois ans et que les résultats de cet audit soient publiés. Le premier audit de ce cycle aura lieu en 2012.

liste des pays Wassenaar: pourquoi certains Suisses de l'étranger ne peuvent-ils pas voter par Internet ? Il faut ici dissiper une erreur fréquemment entendue quant à l'accès des Suisses de l'étranger au vote électronique. Seuls les expatriés vivant dans l'Union européenne ou dans l'un des États signataires de l'arrangement de Wassenaar reçoivent un matériel de vote leur permettant de voter en ligne. Cela n'a rien à voir avec la nature des applications de vote par Internet utilisées en Suisse (open source ou non); il s'agit d'une décision de la Confédération qui obéit à une logique juridique.
En ratifiant l'arrangement de Wassenaar, les États s'engagent à ne pas punir le commerce de biens et services dits à double usage, civil et militaire. Les applications cryptographiques font partie de ces biens et services. En restreignant l'accès au vote en ligne aux Suisses vivant dans un pays qui s'est engagé à ne pas poursuivre en justice les utilisateurs de tels biens et services - car c'est de cela qu'il s'agit - Berne a voulu protéger d'éventuelles poursuites judiciaires ses ressortissants qui vivent hors de ces pays.

sel: le salage consiste à ajouter une chaîne de caractères à l'information avant le hachage.