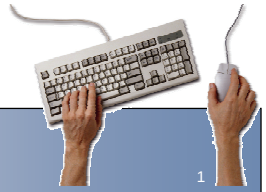
"Le vote par internet doit être au moins aussi sûr que le vote postal"

(Le Conseil fédéral)

Pas de problème, il l'est beaucoup plus!

(Genève)

Michel Warynski
Michel Chevallier
Chancellerie d'Etat, Genève



Introduction

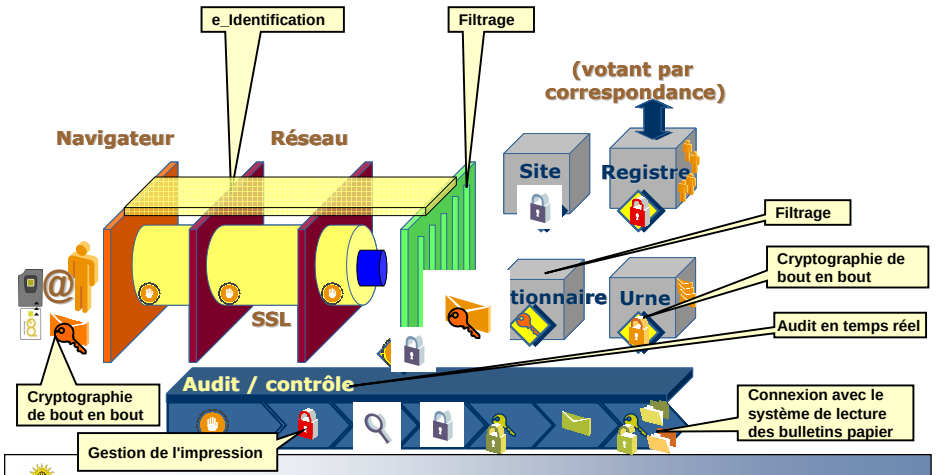
- L'injonction du Conseil fédéral fournit un benchmark utile au vote en ligne
- L'absence de contrôle par l'Etat sur le bulletin de vote jusqu'à son arrivée dans les locaux de l'administration est la grande faiblesse du vote postal
- Avec le vote par internet, nous sommes meilleurs que le vote postal sur de nombreux aspects
- A Genève, nous avons d'abord conçu une plateforme hautement sécurisée, puis nous y avons implanté l'application métier (le vote)

Le système genevois de vote en ligne

- **Simple**
  1. Identification
  2. Bulletin de vote
  3. Authentification
  4. Confirmation du vote
- **Ethique**
  - Ségrégation des tâches entre l'équipe technique et la commission électorale
  - Transparent: 85% des logiciels utilisés sont en open source, le reste appartient à l'Etat
  - Les clés de cryptage sont partagées entre plusieurs propriétaires
  - La communication est chiffrée par un clé générée par un générateur de nombre purs (génération quantique)
- **Tous les niveaux ont été renforcés**
  - Niveau applicatif, système d'exploitation, hardware et réseau

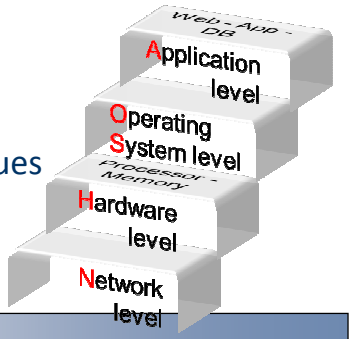
Une architecture performante

Standards – Precision - Performance

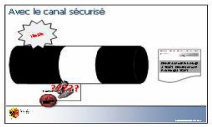


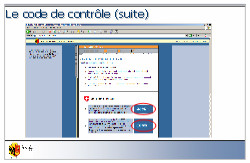
Renforcé à tous les niveaux

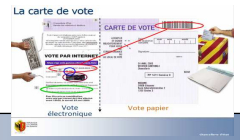
- Les composants que nous utilisons offrent de nombreuses fonctionnalités inutiles dans le cadre du vote
  - **Nous les désactivons**
- Les interactions entre composants sont bloquées
- Le filtrage applicatif ne laisse passer que les commandes et actions prévues par la procédure de vote



Trois spécificités

- Notre application a trois spécificités qui ne se retrouvent pas ailleurs:
  - Le canal sécurisé 

  - Le code de contrôle 

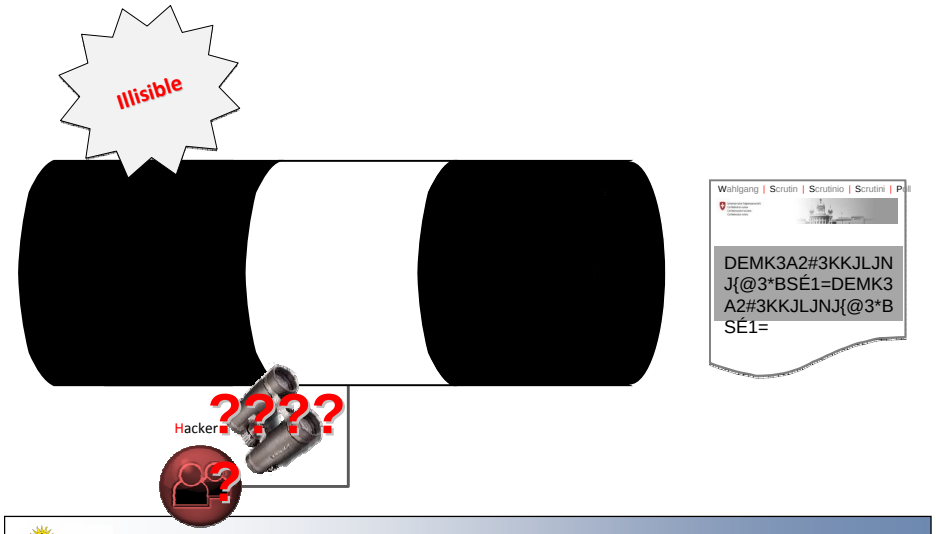
  - L'existence d'une identité physique 

Le canal sécurisé

- Le protocole SSL est doublement vulnérable:
  - Parce qu'il est activé par le navigateur, lequel peut être facilement compromis
  - Parce qu'il peut être cassé
- Le canal sécurisé (applet java) remplit une triple fonction:
  - Il fournit une encryption supplémentaire à celle du SSL, sans lien avec le navigateur
  - Il contrôle la cohérence des messages reçus des utilisateurs
  - Il tient à distance les malwares que votre PC pourrait contenir
- La clé d'encryption de ce canal est formée de nombres aléatoires purs, générés par un générateur quantique

Avec le SSL seul

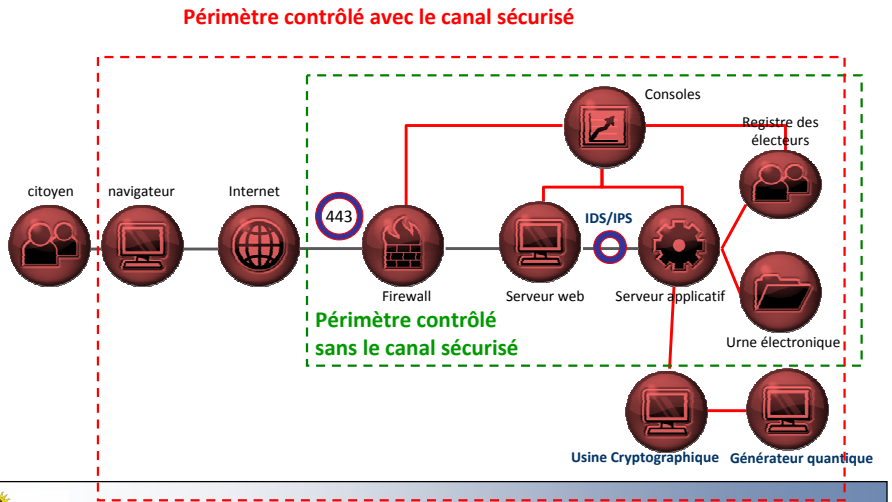
Avec le canal sécurisé



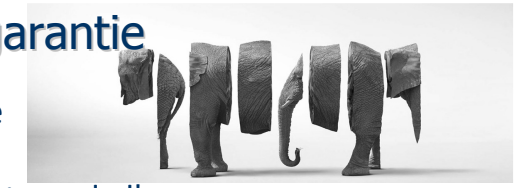
Un large périmètre contrôlé

- La force du vote au local réside dans le contrôle total par l'Etat du lieu où se déroulent le vote et le dépouillement
- Le vote postal affaiblit ce contrôle
- Le canal sécurisé rétablit le contrôle de l'Etat
- Par rapport au schéma standard du vote par internet, le canal sécurisé permet d'étendre le périmètre que nous contrôlons
- Il recrée des conditions proches de celles du vote au local

Un large périmètre contrôlé: illustration



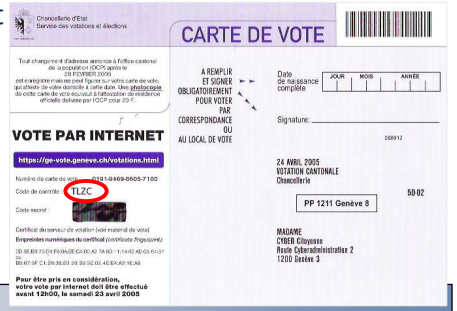
Intégrité de l'urne garantie



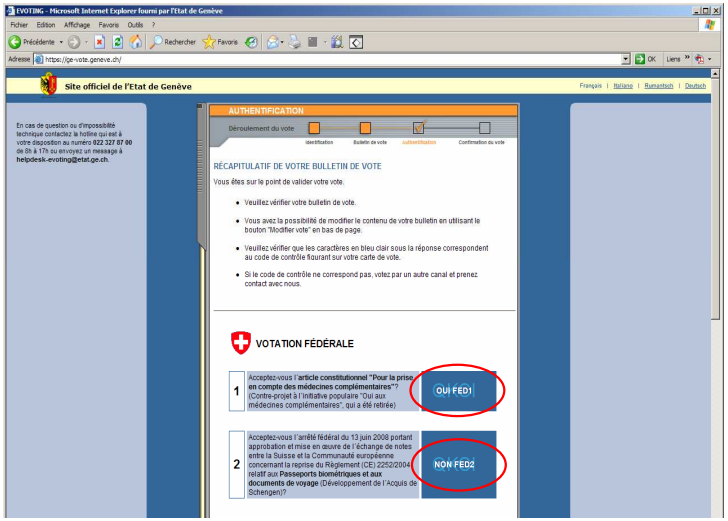
- Le contrôle de cohérence permis par l'applet java garantit l'intégrité du contenu de l'urne
  - Nous avons l'assurance que son dépouillement est possible
  - Nous avons l'assurance qu'elle ne contient pas d'incohérences
- Un second contrôle est fourni par l'urne de test
  - La commission électorale détient les clés de l'urne électronique (ségrégation de devoirs)
  - Ses membres votent dans une commune fictive qui leur est réservée et notent leur votes
  - Le dépouillement de cette commune permet de vérifier la conformité des résultats avec l'input

Le code de contrôle

- Le code de contrôle remplit deux fonctions
  - Il confirme à l'électeur que celui-ci vote bien sur le site de l'Etat
    (Nous savons tous que rares sont les utilisateurs qui vérifient le certificat du site)
  - Il nous permet d'enfouir les réponses des électeurs dans une capsule-image afin de les protéger encore plus lors de leur transit sur internet
- Ce code est propre à chaque citoyen
- Il change à chaque scrutin
- Il figure sur la carte de vote



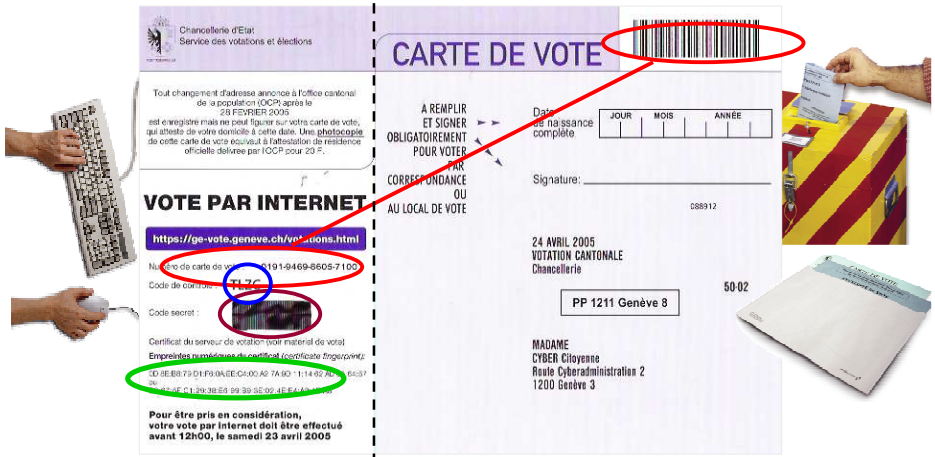
Le code de contrôle (suite)



L'identité physique

- Il est tentant d'utiliser un token dérivé de la norme X509 pour identifier l'électeur
- Cela apporterait cependant plus de problèmes que de solutions
  - Délégation au navigateur du contrôle d'identité
  - Impossibilité de savoir qui est véritablement derrière le PC client
- Nous avons opté pour une solution classique: combiner quelque chose que l'électeur possède
  (le code PIN de sa carte de vote)
  avec des information qu'il connaît
  (sa date de naissance et sa commune d'origine

La carte de vote



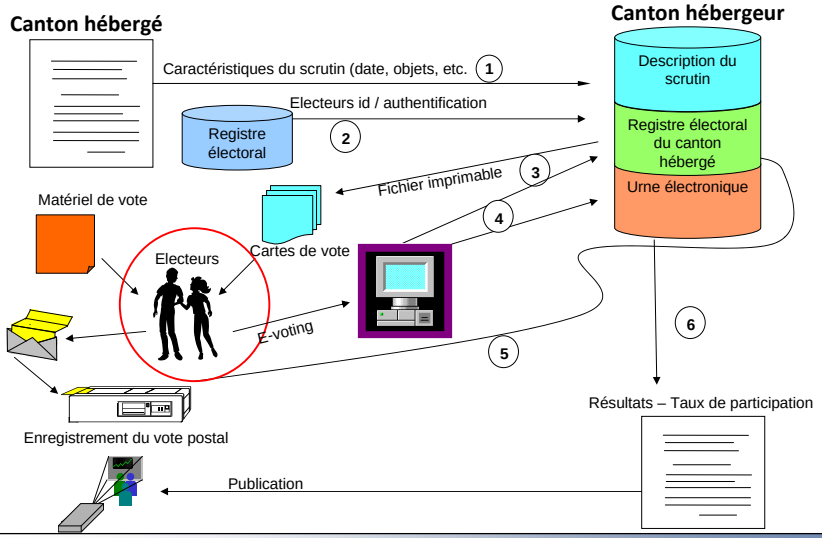
Quelques autres mesures, en vrac

- Cette énumération n'est pas exhaustive
- Il est possible de mentionner encore :
  - L'absence de lien entre urne électronique et registre électoral
  - Le fait que ce registre est totalement anonyme et ne contient que les No des cartes de vote
  - L'urne contient un compteur de votes crypté, qui n'est pas accessible à l'administrateur de bases de données
  - Ce compteur permet de s'assurer en fin de scrutin qu'aucun ajout ou suppression de vote n'a eu lieu
  - Manipuler le contenu des votes est impossible: la clé de cryptage de l'urne est aux mains de la commission électorale
  - Le contenu de l'urne est brassé avant d'être décrypté
  - Etc.

L'hébergement

- La conception de notre plateforme offre une grande souplesse quant aux applications qui peuvent y tourner
- C'est pourquoi nous avons émis l'idée d'héberger les électeurs des cantons intéressés
- Nous signerons avec Bâle-Ville à la fin du mois
- Berne, Lucerne et Uri son les suivants sur notre liste

L'hébergement en images



"Une nouvelle vérité scientifique ne triomphe pas en convaincant ses opposants et en leur faisant voir la lumière, mais parce que ses opposants finissent par mourir et une nouvelle génération arrive qui est familière avec elle."

Max Planck
(1858- 1947)

Merci de votre attention

www.ge.ch/evoting

michel.warynski@etat.ge.ch

michel.chevallier@etat.ge.ch