

CH*✓*ote

Voter par internet

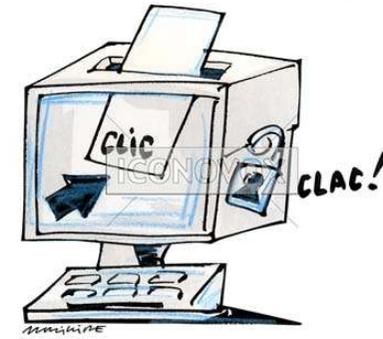
Le système genevois

Le vote en Suisse



- 4 votations par année sur des sujets fédéraux, cantonaux et communaux (initiatives, référendums).
- Elections régulières des représentants politiques à ces 3 niveaux.
- 3 possibilités : à l'urne, par correspondance, par internet.
- Le matériel de vote est envoyé à chaque citoyen ayant le droit de voter.
- Le vote par internet nécessite une inscription préalable.
- La carte de vote donne les codes nécessaires pour accéder au vote par internet : codes de vérification, code de confirmation, code de finalisation.

La procédure de vote



- Le citoyen se connecte au système au moyen des données d'authentification.
- Le citoyen saisit son vote et l'envoie dans l'urne électronique au moyen des données d'authentification.
- Le citoyen se voit confirmer que le vote exprimé a bien été enregistré dans l'urne électronique et qu'il n'a pas été modifié.





Chancellerie d'Etat
Service des votations et élections

FED-CAN



CARTE DE VOTE

1000100



28 février 2016
VOTATION POPULAIRE
Local fictif Electeurs de Test

P.P. CH - 1211
Genève 26

Poste CH SA

99-01

Monsieur
CYBER Citoyen
Route Cyberadministration 1
1200 Genève 3



Tout changement d'adresse annoncé à l'office cantonal de la population et des migrations (OCPM) après le 24 NOVEMBRE 2015

est enregistré mais ne peut figurer sur votre carte de vote, qui atteste de votre domicile à cette date. Une **photocopie** de cette carte de vote équivaut à l'attestation de résidence officielle délivrée par l'OCPM pour 25 F.

VOTE ÉLECTRONIQUE

Pour être pris en considération, votre vote électronique doit être effectué avant 12h00, le samedi 27 février 2016

<https://demo.evote-ch.ch/ge>

Numéro de carte de vote: **7126-9534-7834-7671** 1

Empreintes numériques du certificat (certificate fingerprint):

4B:DA:9E:E8:3A:B3:3D:02:E6:5D:3F:30:F3:B6:E6:EF:
B0:5E:B8:82:57:3A:1B:2B:5C:32:18:AE:EB:D3:82:0F
ou
B7:2E:00:D9:80:78:47:AE:72:3B:81:81:A7:27:F8:33:C6:69:98:5F

A REMPLIR ET SIGNER OBLIGATOIREMENT
POUR VOTER PAR CORRESPONDANCE
OU AU LOCAL DE VOTE

Date de naissance complète

JOUR		MOIS		ANNÉE	

Signature: _____

Code de confirmation:



Grattez avec une pièce de monnaie

Code de finalisation: **897572** 3

Le processus technique



- Préparation des données d'authentification client, des clés cryptographiques et des autres paramètres du système.
- Informations et soutien aux électeurs et aux vérificateurs.
- Préparation et impression du matériel de vote.
- Ouverture et fermeture du canal de vote électronique.
- Contrôle de la conformité et enregistrement des suffrages définitifs.
- Dépouillement de l'urne électronique.

Les bases légales



- **Des ordonnances fédérales fixent les conditions pour autoriser une administration à utiliser le vote électronique :**
 - Le système garantit la sûreté et la fiabilité du vote.
 - Le système est facile à utiliser pour les électeurs.
 - Toutes les opérations techniques et organisationnelles qui sont pertinentes du point de vue de la sécurité doivent être documentées de manière compréhensible.
- **Une base légale genevoise fixe les exigences :**
 - Rendre public le code source des applications du vote électronique, renforçant ainsi sa transparence et son contrôle démocratique.
 - Tester fréquemment la sécurité du système.
 - Auditer le système au moins une fois tous les 3 ans. Les résultats de l'audit sont rendus publics. La portée de l'audit n'est toutefois pas précisée.

Les objectifs de sécurité



- Garantir l'exactitude du résultat.
- Protéger le secret du vote et interdire l'établissement de résultats partiels de manière anticipée.
- Assurer la disponibilité des fonctionnalités.
- Protéger les informations personnelles concernant les électeurs.
- Protéger contre les manipulations les informations destinées aux électeurs.
- Interdire l'établissement de preuves relatives au comportement du vote.

Les nombreuses menaces (risques)



- Un attaquant lit, détourne, modifie, crée, détruit des suffrages.
- Un administrateur manipule les suffrages.
- Un administrateur consulte de manière anticipée des suffrages.
- Une attaque DOS rend le système indisponible.
- Un attaquant pénètre dans le système pour falsifier le résultat.
- Un logiciel malveillant modifie le suffrage sur la plateforme de l'utilisateur.

La vérification est donc indispensable



- Vérification individuelle

- Chaque électeur doit avoir le moyen de contrôler que :
 - son vote a été transmis au système contenant l'urne officielle,
 - son vote n'a pas été modifié.

- Vérification complète

- Les vérificateurs doivent recevoir la preuve attestant que les résultats ont été établis correctement :
 - Tous les suffrages enregistrés dans l'urne électronique ont été pris en compte,
 - Et uniquement ces suffrages.



Les objectifs d'audits



- Analyse des vulnérabilités et tests d'intrusion.
- Analyse du code.
- Analyse des mesures mises en œuvre pour garantir la sécurité du système.
- Analyse de l'ergonomie du système.

Analyse des vulnérabilités et tests d'intrusion

- A faire par des spécialistes car :
 - Il faut connaître toutes les techniques d'attaque existantes.
 - Il faut connaître les vulnérabilités de l'infrastructure logicielle utilisée.
 - Il faut savoir exploiter les vulnérabilités trouvées.

Résultat de l'analyse

- Pas de vulnérabilités exploitables :
 - Les meilleures pratiques en matière de maintenance et d'exploitation des infrastructures sont respectées.
- Pas d'intrusion réussie.



Analyse du code



Résultat de l'analyse

- Le code source est disponible sur internet.
- Licence open source par la Free Software Foundation.
- L'Etat de Genève encourage les communautés d'informaticiens à contribuer à l'amélioration du code source.
- L'audit du code devient ainsi inutile.

Analyse des mesures mises en œuvre pour garantir la sécurité du système

- Organisation opérationnelle
 - Identification et évaluation des risques
 - Mesures organisationnelles réduisant ces risques
 - Ségrégation des rôles
 - Sécurité des accès (physiques, logiques)
- Gestion informatique
 - Contrôles généraux informatiques (COBIT)
 - Détection et gestion des incidents
 - Gestion de la performance et de la disponibilité
 - Plans de secours



Analyse des mesures mises en œuvre pour garantir la sécurité du système

Résultat de l'analyse

- Améliorer la ségrégation des rôles
 - Contrôle des journaux applicatifs à faire par un externe à l'équipe de développement afin de détecter les possibles anomalies ou abus.
 - Formaliser une liste des rôles ayant accès au serveur de fichiers.
 - Administrateurs des serveurs ne doivent pas vérifier la configuration de la sécurité des serveurs.
- Améliorer la documentation des processus
 - Les personnes qui surveillent les processus n'ont pas une connaissance suffisante de l'utilité des actions et contrôles qu'elles font.
- Améliorer la sécurité des serveurs
 - Mieux sécuriser le contrôle des accès aux systèmes qui gèrent le e-voting.
 - Limiter les accès privilégiés aux serveurs gérant le vote électronique.

Analyse de l'ergonomie du système

- Le système doit être efficace et facile d'utilisation
 - Malgré les étapes d'authentification, de validation et de vérification qui nécessitent la saisie et la vérification de codes.
 - Logique du système = logique de l'utilisateur.
- Le système doit inspirer confiance au votant
 - Sécurité et secret du vote.
- Le système ne doit pas influencer l'opinion du votant.
- L'utilisateur doit pouvoir modifier son vote jusqu'à la validation.



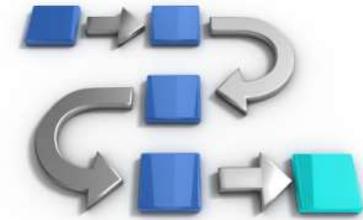
Analyse de l'ergonomie du système

Résultat de l'analyse

- Explication plus claire de l'utilité des différents codes à saisir ou à vérifier (codes **1** , **2** , **3** , cf. dia 4)
 - Renforce la perception de la sécurité du vote, donc l'adoption du système par le votant.
- Améliorer la visibilité des étapes de la procédure de vote en cours d'exécution.
- Améliorer la visibilité de la documentation pdf des objets de la votation.
- Améliorer le repérage des codes de vérification sur la carte de vote pour chaque étape de la procédure de vote.



Conclusion



- Bonne qualité et sécurité du système genevois.
- Audits indépendants à mener régulièrement pour que le citoyen ait confiance dans ce système.
- Audits techniques et complexes (grande visibilité, beaucoup d'exigences, risques nombreux et impacts importants).

