Date de dépôt : 13 août 2013

Rapport

de la Commission des droits politiques et du règlement du Grand Conseil chargée d'étudier le rapport du Conseil d'Etat au Grand Conseil sur l'audit triennal du système genevois de vote électronique

Rapport de M. Jean-Marie Voumard

Mesdames et
Messieurs les députés,

La Commission des droits politiques et du règlement du Grand Conseil, lors de ses séances des 15 et 22 mai 2013, a étudié le rapport sur l'audit triennal du système genevois de vote électronique.

Cet objet a été étudié sous la présidence de M. Serge Hiltpold.

M[me] Irène Renfer, secrétaire scientifique/SGGC, et MM. Fabien Waelti et David Hofmann, directeur et directeur suppléant des affaires juridiques / Chancellerie, étaient présents lors de ces séances.

Les procès-verbaux ont été tenus par M[me] Tina Rodriguez et M. Gérard Riedi.

Qu'ils soient ici remerciés pour la qualité de leur travail.

Présentation du RD 983 par M[me] Anja Wyden Guelpa, Chancelière d'Etat, et M. Michel Warynski, directeur du support et des opérations de vote

En présence de MM. Eric Favre, directeur général de la DGSI, et Jean-Pierre Gilliéron, directeur sécurité

M[me] Wyden Guelpa annonce que l'art. 60 al. 6 de la LEDP prévoit que le Conseil d'Etat doit faire auditer, au moins une fois tous les trois ans, la plateforme de vote électronique. Il doit ensuite rendre publics les résultats.

ATAR ROTO PRESSE – 300 ex. – 09.13

La période des trois ans est arrivée à échéance l'année dernière. Il convient donc d'analyser les résultats des trois audits qui ont été réalisés. Il est à noter que la commission électorale centrale (CEC) a été consultée et impliquée dans la réalisation de l'audit, tout comme la direction générale des systèmes d'information (DGSI). Ces deux entités ont permis la définition du périmètre de l'audit.

Il convient de distinguer le contrôle des procédures de sécurité, d'une part, et les tests d'intrusion, d'autre part. L'audit est une manière d'avoir un dialogue avec les partis politiques et permet une amélioration continue.

Il a été décidé de faire un seul audit en trois volets afin d'avoir une image claire et précise. Un premier audit, test d'intrusion, a été retenu. Il convenait, à travers ce test, de voir si les différents serveurs résistaient aux différentes tentatives d'intrusions. Un audit du code des fonctions cruciales du système a été mis en place. Cela concernait plus particulièrement le dépouillement des votes et de l'urne. Finalement, une certification ISO 9001 de la préparation, de la gestion et du suivi du canal électronique des scrutins, a été réalisée. Pour la première fois, une analyse du code a été faite par une société externe à l'Etat. Des entreprises « neutres » ont été choisies, pour ce faire.

M. Gilliéron annonce que le test d'intrusion porte sur le hardware du vote électronique et les logiciels permettant son fonctionnement face aux intrusions depuis internet et depuis un PC de l'Etat.

M. Gilliéron annonce que les résultats ont été bons puisqu'aucun point négatif n'a été relevé. Les services exposés sont à jour sur internet, ce qui est très important. Des mises à jour sont réalisées régulièrement afin d'éviter que le système ne soit piraté.

Pour l'analyse du code, les fonctionnalités les plus sensibles ont été sélectionnées et la norme ISO 25 000 a été prise en compte. Le coût de cet audit s'élève à 152 488 F, correspondant à 36 jours de travail.

Concernant le résultat de l'analyse de code, l'auditeur a constaté que sept exigences de sécurité définies par l'administration étaient implémentées selon les bonnes pratiques et seules quatre vulnérabilités ont été identifiées. L'auditeur a fait des propositions afin d'atteindre une qualité de 100% sur les neuf exigences, appelées « commandements fondateurs ». Les vulnérabilités ont été corrigées pour la votation du 3 mars 2013.

M^{me} Wyden Guelpa déclare qu'une analyse ISO a été réalisée. Elle portait sur la qualité de l'ensemble du scrutin. L'auditeur considère que la certification externe pourrait être obtenue très rapidement. Les résultats sont donc très positifs.

Le parti pirate et la haute école de gestion bernoise ont demandé cet accès et vont également publier leur regard sur le système. Ce renforcement de la transparence est bénéfique, selon M^me^ Wyden Guelpa.

Pour l'instant, le code ne peut être publié, dans un souci de confidentialité. Les personnes ayant accès au code ont signé une charte de confidentialité. Elles n'ont pas été sous la surveillance d'un collaborateur ou d'une autre personne car il a été décidé qu'il était préférable de leur faire confiance.

La CEPP a été mandatée par le Conseil d'Etat pour évaluer la pertinence du vote électronique. Un rapport sera publié avant la fin du mois de mai.

Sur les audits, les mesures de sécurité mises en place ont été validées. Il convient de rappeler que le risque zéro n'existe pas mais les audits confirment que la plateforme est gérée de manière dynamique et adaptée.

M^me^ Wyden Guelpa explique qu'actuellement, le système genevois a été repris par trois cantons. Ils seront bientôt cinq cantons à l'utiliser. Plusieurs groupes d'utilisateurs font valoir les modifications qu'ils souhaitent. Ce mécanisme permet de connaître les différentes sensibilités et diversités, ce qui est très enrichissant.

M. Warynski déclare que les autres cantons ne connaissent pas la notion de commission électorale. Ils ne peuvent donc effectuer les mêmes contrôles qu'à Genève. Une urne de contrôle est par contre régulièrement demandée. Cette dernière consiste à mettre en place un local de vote virtuel dans une commune virtuelle avec des votants fictifs. La commission électorale effectue des votes, au nom de ces citoyens, et les votes sont ensuite protocolés. Finalement, un contrôle est effectué pour analyser les résultats du local de vote virtuel, en comparaison avec ce qui a été protocolé, pour voir si les résultats sont en adéquation. L'urne de contrôle peut différer selon les cantons et leurs spécificités.

Pour Genève, l'utilisation du vote électronique par les expatriés est de l'ordre de 45 à 47% (la plupart sont des frontaliers). En ce qui concerne les résidents, les pourcentages sont de l'ordre de 15 à 21%, ce qui n'est pas énorme mais l'utilisation du vote par correspondance a augmenté très largement. L'introduction du vote électronique ne fera pas nécessairement exploser la participation genevoise.

La participation est déjà bonne, en comparaison de la participation au niveau fédéral. Genève a toujours une participation 5% plus élevée que la participation au rang fédéral.

Il convient d'admettre que la société effectue de nombreuses opérations par internet actuellement et il faudra donc s'adapter en conséquence, pour maintenir ce bon taux de participation.

Prise de position des groupes

Une députée (L) a entendu aujourd'hui à la radio que le vote électronique n'avait pas atteint ses buts. Il a éventuellement permis de conserver le vote des jeunes qui sont habitués à ce système, mais la chancelière disait dans le journal qu'il fallait penser à une application pour smartphone ou tablette. C'est un peu décevant. En effet, elle pensait que le vote électronique allait faciliter la vie des jeunes votants, ce qui n'est apparemment pas le cas.

Le Président avait aussi relevé que la demande importante visait les Suisses de l'étranger. En effet, il y avait pas mal de problèmes avec le vote par correspondance. Un autre élément souligné était l'espoir de conserver la part de votants chez les jeunes. Maintenant, hormis le contexte idéologique des partis, c'est un service pour la population qui semble nécessaire.

Un député (Ve) fait remarquer, par rapport aux commentaires effectués, que les Verts étaient sceptiques par rapport au vote par internet. Maintenant, certains éléments vont dans le bon sens, notamment le fait que le code source ait été ouvert et ait pu être consulté par la haute école de gestion bernoise et par le parti pirate. La direction prise consistant éventuellement à ouvrir complètement le code serait ainsi très positive. Par rapport à ce regard extérieur, il conserve des critiques, mais celles-ci sont difficiles à résoudre. Quand une personne vote dans un local de vote ou par la poste, même sans savoir effectivement ce qu'il se passe après, elle peut comprendre où peuvent se trouver les failles si on lui explique le principe et le fonctionnement des procédures. Ce député (Ve) ne doute pas de la validité de l'étude sur le vote par internet, mais on est un peu dépossédé de la procédure. Des gens disent ainsi que ce qui se passe dans le « bidule » se passe bien sans que les commissaires sachent vraiment ce qu'il en est. Ce député (Ve) pense qu'il va être demandé de plus en plus aux partis d'avoir des gens qui sont compétents dans le domaine de l'informatique et qui les représentent dans la commission électorale. Cela sera un enjeu important à l'avenir. Tant que tout va bien – c'est le cas pour l'instant – et que cela reste à un niveau local, les enjeux sont peu importants. On voit mal des gens pirater les votes afin de faire pencher la balance dans un sens ou l'autre. En revanche, lorsqu'il y aura des enjeux nationaux, hautement politiques ou avec de grands enjeux financiers, il faudra être sûr que le système est valable à 100 %, sinon il y aura sans arrêt des gens qui pourront penser qu'il y a eu manipulation lorsque les résultats sont très serrés puisqu'il n'y a aucune trace des bulletins.

Un député (UDC) assimilait ce rapport à quelqu'un qui porterait un pantalon avec des bretelles, une ceinture et les mains dans les poches afin de s'assurer que celui-ci ne tombe pas. Le rapport et les audits effectués sont ainsi rassurants. Il semblait exagéré d'effectuer trois audits, mais ils ont été effectués sur des objets différents. Dans l'idée d'avoir une conscience tranquille en matière de vote électronique, le rapport et les explications de la chancelière ont permis de rassurer les commissaires.

Un député (MCG) estime que ce rapport est très bon. Pour autant, le risque zéro n'existe pas, quel que soit le mode de vote. Si quelqu'un est malveillant, il peut toujours le faire. Cela étant, internet est l'avenir. Le groupe MCG est ainsi favorable au RD 983 et au développement de la plateforme de vote par internet.

Un député (Ve) confirme que le risque zéro n'existe pas. Toutefois, le principal problème du vote par internet est qu'il est plus facile de modifier l'ensemble des votes que de le faire dans un local de vote et sur l'ensemble du canton. En plus, dans un local de vote, on retrouve les bulletins quelque part. Pour le vote par internet, les possibilités de vérification ne sont pas les mêmes.

Le Président note, par rapport au développement de cette plateforme, l'intérêt porté par six autres cantons. Finalement, les buts ont été remplis et cela a servi dans une vision intercantonale avec la participation d'autres cantons. Par ailleurs, le Président constate également que ce système de vote est utilisé à 45 % sur les expatriés.

Le Président met aux voix la prise d'acte sur le RD 983.

Pour :	Unanimité (2 S, 3 Ve, 1 PDC, 2 R, 3 L, 1 UDC, 2 MCG)
Contre :	–
Abstention :	–

La prise d'acte est acceptée à l'unanimité.

Les députés de la Commission des droits politiques se déclarent ainsi satisfaits du rapport.

La commission prend acte de ce document à l'unanimité.

La commission propose au Grand Conseil de suivre sa décision et vous demande de prendre acte du RD 983.

ANNEXE

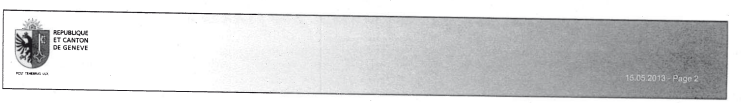
Premier cycle d'audits triennaux de la plateforme genevoise de vote électronique

Présentation à la Commission
des droits politiques
du Grand Conseil
15 mai 2013

Anja Wyden Guelpa, Chancelière d'Etat

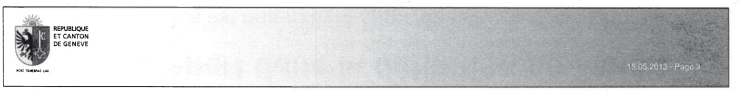
A l'origine, un vote de votre Conseil

- En 2009, votre Conseil a adopté le PL 9931
- Celui-ci a introduit dans la Loi sur l'exercice des droits politiques (LEDP, A 5 05) un article 60, dont l'alinéa 6 dit notamment que le Conseil d'Etat fait auditer au moins une fois tous les 3 ans la plateforme de vote électronique et rend publics les résultats
- Cet article, rédigé par votre commission, est entré en vigueur le 1er janvier 2010
- La première période de 3 ans a pris fin au 31 décembre 2012
- Nous vous présentons aujourd'hui les résultats de ce premier cycle d'audits triennaux



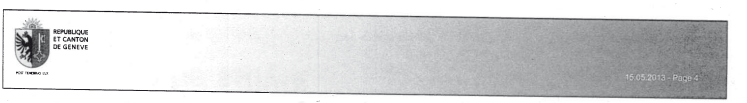
La démarche suivie

- L'article 48 de la Constitution en vigueur jusqu'à fin mai institue une Commission électorale centrale (CEC)
- Son rôle est défini à l'article 75B LEDP: la CEC contrôle notamment "la régularité du vote électronique, ainsi que le fonctionnement des moyens techniques" utilisés lors des opérations électorales
- Nous avons associé la CEC à la définition du périmètre de l'audit triennal, lequel correspond à la mise à l'épreuve du "fonctionnement des moyens techniques utilisés" dans les opérations électorales
- La Direction générale des systèmes d'information (DGSI), a également été associée à la définition de ce périmètre en tant que responsable de la solution, de son exploitation et du pilotage de 2 des 3 volets de cet audit.



Point de départ dans la définition de l'audit

- Notre réflexion s'est notamment appuyée sur une distinction que votre commission avait faite lors de l'examen du PL 9931
- Il s'agit de la distinction entre le contrôle des procédures de sécurité, d'une part, et les tests d'intrusion, d'autre part
- Votre commission avait également indiqué que les audits triennaux pouvaient consister en un test d'intrusion, mais pas seulement
- Par ailleurs, dans une optique d'amélioration continue, 4 tests d'intrusion avaient déjà été réalisée sur la plateforme genevoise de vote électronique avant le présent audit.
- Dès lors, nous avons réfléchi à un audit pluriel qui intègre différentes dimensions



Les choix retenus

- En accord avec la CEC et la DGSI, la chancellerie d'Etat a abordé la sécurité du vote électronique sous plusieurs angles
- Au final, les audits suivants ont été retenus:
  - Un test d'intrusion destiné à vérifier que le réseau dédié au vote électronique, les pare-feu filtrant l'accès aux serveurs et les logiciels reliant les différents éléments d'infrastructure résistent aux tentatives d'intrusion
  - Un audit du code des fonctions cruciales du système (identification du votant, dépôt du vote et dépouillement de l'urne électronique)
  - Une certification ISO 9001 de la préparation, de la gestion et du suivi du canal électronique des scrutins. Par cette certification, la chancellerie a voulu mettre à l'épreuve son organisation
- Aucune analyse de code par une société externe à l'Etat n'avait jamais été faite sur notre système, c'est donc une première

Le choix des mandataires

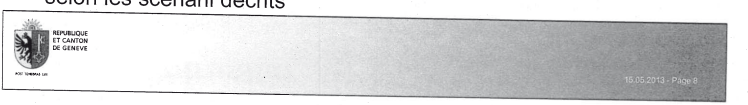
- Les mandataires ont été choisis par la DGSI (test d'intrusion et audit de code) et la Chancellerie (certification ISO 9001) sur la base d'appels d'offre sur invitation
- Seules des sociétés n'ayant jamais travaillé sur le vote électronique ont été invitées à soumissionner dans ce cadre
- Il s'agit d'éviter des biais liés à une expérience préalable dans l'abord de la plateforme de vote par les auditeurs

Le test d'intrusion

- Le test d'intrusion a porté sur les points suivants:
  - Le hardware du vote électronique et les logiciels qui le font fonctionner sont-ils vulnérables aux intrusions depuis internet?
  - Le hardware du vote électronique et les logiciels qui le font fonctionner sont-ils vulnérables aux intrusions depuis un PC de l'Etat?
  - Peut-on, depuis un PC de l'Etat, pénétrer le réseau protégé utilisé pour le vote électronique?
- Des cartes de vote et un compte utilisateur sur les PC de l'Etat ont été fournis à l'auditeur

Résultats du test d'intrusion

- L'auditeur a relevé 4 points positifs et aucun point négatif
  - La surface d'attaque depuis internet est correctement limitée (*depuis internet, la plateforme de vote n'expose que ce qui est strictement nécessaire au bon déroulement de sessions de vote*)
  - Les entrées du votant sont correctement traitées (*les requêtes reçues par le système lors des sessions de vote sont canalisées et filtrées de manière à prévenir des actions non souhaitées*)
  - Les services exposés sur internet sont à jour (*les logiciels visibles depuis internet sont mis à jour, notamment quant aux corrections de sécurité*)
  - La segmentation du réseau et le filtrage des flux vers le réseau du système de vote électronique sont excellents
- Les réponses aux questions posées dans la diapositive précédente sont négatives; il n'est pas possible de compromettre la plateforme selon les scénarii décrits



L'analyse de code

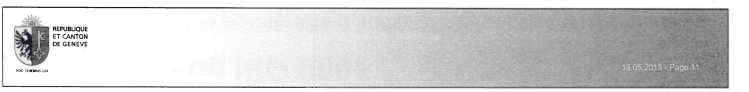
- Le code du vote électronique compte 75'000 lignes; c'est pourquoi nous avons sélectionné les fonctionnalités les plus sensibles
  - L'identification du votant
  - Le dépôt du vote, comprenant
    - L'authentification du votant
    - La réception, le déchiffrement et le contrôle du bulletin chiffré
    - Le chiffrement et le stockage du bulletin validé dans l'urne électronique
  - Le dépouillement de l'urne électronique, comprenant
    - Le brassage et le déchiffrement des bulletins
    - La comptabilisation et la consolidation des bulletins
    - L'édition des résultats
- Le référentiel utilisé a été bâti sur la norme ISO 25'000 (*Exigence et évaluation de la qualité des produits logiciels*)
- l'auditeur a comparé les objectifs de sécurité de l'administration à leur traduction dans le code

Résultats de l'analyse de code

- L'analyse a été menée sur 2 axes
  - Un audit systématique du code centré sur les 9 exigences de sécurité
  - La vérification que les parties sensibles du code ont été implémentées selon les meilleures pratiques de sécurité
- L'auditeur a constaté
  - que 7 exigences de sécurité définies par l'administration sont implémentées selon les bonnes pratiques
  - que 4 vulnérabilités ont été identifiées, concernant 2 des exigences
- L'analyse approfondie de ces 4 vulnérabilités par l'auditeur a précisé
  - que l'impact de 3 d'entre elles est nul sur l'application
  - que l'utilisation de la 4e nécessiterait des accès hautement privilégiés à 2 ressources internes différentes du système d'information du vote électronique durant la période de scrutin

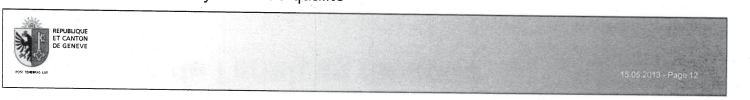
Résultats de l'analyse de code

- A la suite de son analyse l'auditeur a fait des propositions permettant d'atteindre une qualité de 100% sur les 9 exigences
- L'auditeur conclu que 7 des 9 «Commandements Fondateurs» satisfont à 100% aux bonnes pratiques de sécurité et que les recommandations proposées permettraient d'atteindre un niveau de qualité de 100% sur tous les «Commandements Fondateurs»
- Ces propositions ont été implémentées dès le scrutin 3 mars 2013 et leur implémentation a été validée par un second mandataire externe



Le processus ISO 9001

- Pour compléter le portefeuille d'audits 2012, une démarche qualité selon la norme ISO 9001 a été entreprise
- L'objectif final est de mettre en place un système de management de la qualité sur l'ensemble du scrutin (y compris le vote papier)
- Le périmètre de ce système comprend les processus suivants
  - Gouvernance des opérations électorales
  - Gestion des ressources à disposition
  - Opérations de vote
  - Amélioration continue
- L'auditeur a effectué les tâches suivantes
  - Evaluation de la situation
  - Elaboration d'un plan d'action et accompagnement de sa mise en oeuvre
  - Mise en œuvre du système de qualité
  - Vérification du système de qualité



Résultats du processus ISO 9001

- Ce travail de préparation est achevé
- La Direction du support et des opérations de vote (DSOV) de la Chancellerie dispose désormais d'un système de gestion de la qualité
- L'auditeur a conclu que la DSOV peut obtenir rapidement la certification ISO 9001

Conclusion

- Les 3 audits ont livrés des résultats extrêmement positifs
- Ils ont permis de valider l'efficacité des mesures de sécurité mises en œuvre et également de les renforcer dès ce printemps
- Cela confirme le sérieux de la gestion de la plateforme de vote électronique et des scrutins
- Cela confirme aussi que cette plateforme est gérée de manière dynamique et adaptée à l'environnement changeant des technologies de l'information
- Les rapports sont désormais publics sur le site internet de l'Etat

Merci de votre attention