RÉPUBLIQUE ET CANTON DE GENÈVE
Chancellerie d'Etat
SECRÉTARIAT GÉNÉRAL

Information et documentation

Genève, le 4 février 2002

Sécurité du vote par Internet
Le rapport du comité d'experts est désormais disponible

L'application de vote par Internet développée à Genève est un « château fort » quasi inexpugnable, estiment les experts mandatés par la Chancellerie d'Etat pour l'auditer. La fiabilité du poste utilisateur doit néanmoins être améliorée. En accord avec la Confédération, qui supervise ce projet, la Chancellerie a confié à des spécialistes reconnus de nouveaux mandats portant sur ce poste et sur des tentatives de hacking. Le rapport d'experts, déposé à fin janvier 2002, a été transmis pour évaluation au groupe de travail fédéral "Avant-projet Vote électronique", qui réunit la Confédération et les cantons de Genève, Neuchâtel, Zurich, Berne, St-Gall et Tessin. Il est disponible sur le site Internet de l'Etat, www.geneve.ch.

Dans le cadre du projet-pilote de vote par Internet, la Chancellerie a mandaté des collaborateurs du CERN, de l'Université, du Centre des technologies de l'information (CTI) et des Hôpitaux universitaires de Genève pour réaliser une expertise de la sécurité de son application. Ce groupe l'a examinée dans son état au 23 septembre 2001.

Dans son rapport, ce groupe souligne la validité de la démarche et le bon niveau de sécurité de l'application développée par les entreprises mandataires. Cette application est un « château fort » quasi inexpugnable, mais la « forêt » qui l'entoure peut receler quelques surprises. Cette « forêt » représente les postes client, c'est-à-dire les ordinateurs personnels utilisés par les internautes.

Le rapport propose d'accroître la sécurité de la procédure en chiffrant le bulletin électronique de bout en bout à l'aide des clés définies par les contrôleurs des partis, en créant une urne test qui recueillerait leur vote, en prévoyant une connexion automatisée sur le serveur de l'Etat, lequel doit être clairement authentifié, et en brassant les codes d'accès avant chaque votation, ainsi que les bulletins reçus, avant chaque dépouillement, pour garantir leur anonymat. Toutes ces mesures ont été intégrées au prochain test, qui aura lieu dans le cadre des votations du 2 juin 2002, avec un échantillon de quelque 10'000 jeunes.

La sécurité optimale se trouve à l'intersection des deux exigences de sûreté et de confort de l'utilisateur. Plutôt que d'astreindre l'électeur à une discipline qui enlèverait tout attrait au vote en ligne, Genève a opté pour un concept comportant plusieurs couches concentriques de mesures techniques, cryptage, encodage, validation, clé de chiffrement à 128 bits, notamment, garantissant à la fois la sécurité et la simplicité d'utilisation. L'électeur est en outre rendu attentif par une fenêtre automatique à la nécessité de bien identifier le site vers lequel il envoie son vote.

D'entente avec la Confédération, la Chancellerie d'Etat poursuit ses travaux et a confié un nouveau mandat portant sur la sécurisation du poste client dans le respect des nécessités de l'utilisateur, notamment en matière d'accès à l'information électorale. Lors du prochain test, le système fera aussi l'objet de tentatives d'intrusion (hacking) afin d'en tester la robustesse.

République et Canton de Genève

Chancellerie

Cellule sécurité des systèmes d'information

Rapport du Comité Sécurité sur l'application de vote par Internet

Précision au lecteur

Ce rapport est l'oeuvre collective du comité sécurité, présidé par Monsieur Maurice Wenger, responsable de la cellule de sécurité des systèmes d'information de l'Etat, et formé d'experts issus du CERN des Hôpitaux Universitaires de Genève et de l'Université de Genève. Les auteurs de ce rapport n'ont pas jugé relevant que leurs noms soient expressément publiés, ne serait-ce que parce que les institutions pour lesquelles ils travaillent ne sont pas formellement engagées par leurs réflexions, dès lors que leurs structures de direction n'ont pas eu à les valider.

28 janvier 2002

Table des matières

Synthèse pour le lecteur pressé

L'Etat de Genève a fait développer une application de vote par Internet, qui serait utilisée en complément des possibilités existantes (vote par correspondance et dépôt du bulletin de vote dans l'urne), et pour laquelle il désire connaître l'avis de spécialistes en sécurité.

Une lacune dans le chiffrement du vote

Un Comité a été désigné dans ce but, a constaté que cette application, évaluée dans son état de développement au 23 septembre 2001, présente un bon niveau de sécurité pour tout ce qui est sous le contrôle de l'Etat de Genève. Cependant, cette application analysée dans son contexte global, de l'utilisateur à l'urne électronique, ne satisfait pas à plusieurs des onze principes énoncés dans le mandat. Le Comité sécurité propose de remédier à une lacune importante en adaptant l'application pour que le suffrage soit chiffré de bout en bout, donc du poste de travail de l'électeur jusque dans l'urne électronique. Il a fort heureusement déjà été convenu avec les responsables du développement que cette lacune serait corrigée dans la version suivante du prototype.

Le vote par Internet n'implique pas obligatoirement le WEB

Le Comité souligne, par analogie avec l'e-banking (UBS pay, La Poste), que les solutions de vote par Internet ne doivent pas obligatoirement passer par l'utilisation de navigateurs WEB dont la complexité, les failles de sécurité et la diversité posent problème. Une contre-proposition, avec plusieurs variantes, est faite dans ce rapport.

Le poste de l'électeur est le maillon faible

Le maillon le plus faible de la chaîne de vote par Internet est dans la partie hors du contrôle de l'Etat, soit sur l'Internet et chez l'électeur. C'est de ce côté que les premiers efforts d'amélioration de la sécurité doivent porter. Le Comité propose quelques pistes, comme de mettre en place un mécanisme d'authentification forte du serveur qui ne dépende pas de la bonne volonté de l'électeur, ainsi que de fournir à ce dernier un CD-ROM avec le programme de votation. Ce CD-ROM, n'étant pas nécessairement spécifique à la votation, peut être expédié indépendamment du matériel électoral, au cas où les machines de mise sous pli devraient ne pas être adaptées.

Création d'une urne de test

Une application opaque pour le citoyen peut nuire à la crédibilité du système de vote par Internet. Pour améliorer la transparence et la crédibilité, le Comité propose la mise en place d'un mécanisme de test du bon fonctionnement pendant l'opération de vote par Internet. Celui-ci peut consister à créer une urne de test à laquelle n'auraient accès que des personnes de confiance telles que les contrôleurs des partis politiques. Les suffrages de ces personnes de confiance seraient parallèlement traités à la main et, à l'issue de l'opération électorale, les résultats manuels et par Internet devraient concorder. S'agissant de tests, il est évident que les suffrages exprimés dans l'urne de test ne seraient pas comptabilisés dans le décompte final du vote.

1. Mandat

1. Objectifs

L'Etat de Genève a fait développer une application de vote par Internet pour laquelle il désire connaître l'avis de spécialistes en sécurité. Dans ce but, le Chancelier de la République et Canton de Genève a mandaté le CERN, l'Université de Genève (Centre universitaire d'informatique et Division informatique), l'Hôpital cantonal de Genève et l'Etat de Genève (cellule sécurité des systèmes d'information) pour une évaluation de la sécurité de cette application quant au respect de onze principes qu'un vote ou une élection doit satisfaire (Voir annexe). Le présent document constitue le résultat de cette évaluation.

2. Méthodologie

Pour remplir son mandat d'évaluation, le Comité sécurité a auditionné les personnes suivantes :

- M. Jean-Luc Poncet, de Hewlett-Packard ;
- MM. Patrick Ascheri, Gérard Ineichen, Bernard Taschini, Michel Warynski, Daniel Zingg, de l'Etat de Genève.

Il a aussi consulté la documentation du projet et des produits utilisés dans cette application. A ce stade du développement du projet, le Comité n'a pas jugé instructif (par rapport à la charge de travail) de procéder à une analyse exhaustive du code de l'application quant bien même, à sa demande, certaines parties lui ont été soumises.

Pour des questions d'éthique, les membres du Comité n'ont pas essayé d'attaquer l'application depuis leurs entreprises respectives, comme cela avait été envisagé primitivement ; une entreprise spécialisée sera donc mandatée par la Chancellerie pour réaliser ces tests. Il faut également être conscient que ce genre de méthode, si elle peut aboutir à la découverte de vulnérabilités ponctuelles de l'application (qui seraient immédiatement corrigées avec des correctifs logiciels ad hoc), ne permet en revanche pas d'identifier d'éventuelles faiblesses plus générales qui nécessiteraient une révision plus profonde de l'approche choisie.

Le Comité a aussi testé l'opération de vote par Internet lors des tests de septembre.

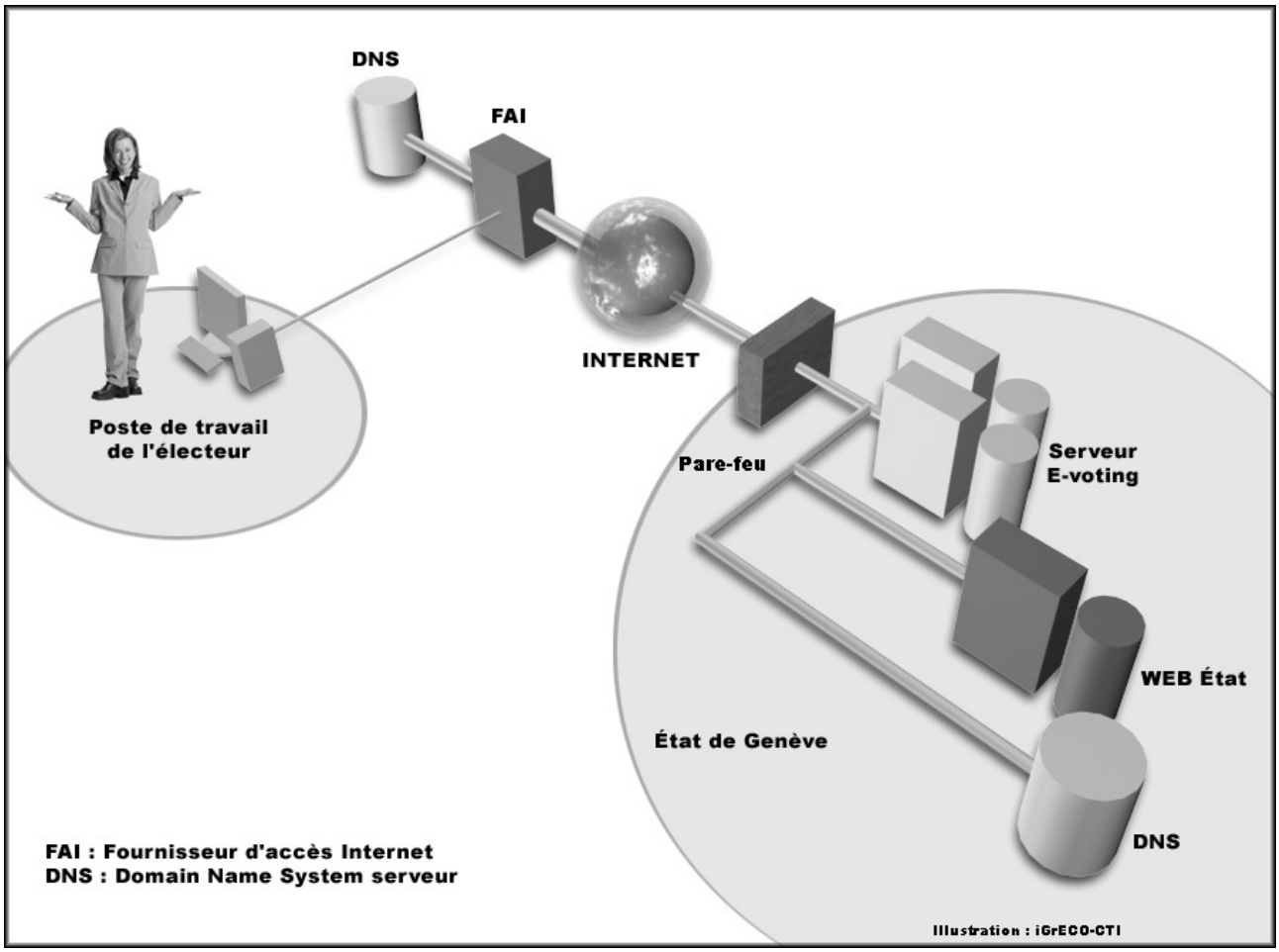
Le Comité, n'ayant pas de compétence particulière en matière d'organisation, a renoncé à faire une validation formelle des procédures écrites qui entourent le fonctionnement de l'application de vote par Internet.

> L'évaluation du Comité et ses commentaires ont trait à l'application, dans ses différents stades d'évolution jusqu'aux tests du 23 septembre, et à son environnement global, depuis l'électeur jusqu'à la sortie des votes déchiffrés.

L'analyse des vulnérabilités a porté sur l'ensemble de la chaîne, de l'électeur jusqu'à la sortie des résultats. Cette analyse n'a fait ressortir qu'une faiblesse majeure, en cours de correction, dans la partie sous le contrôle de l'Etat, les autres vulnérabilités possibles ont été mises en évidence essentiellement dans les éléments de la chaîne hors du contrôle de l'Etat (l'électeur, son poste de travail, Internet,...).

Dans son approche initiale, le Comité avait l'intention de quantifier les risques auxquels est exposée l'application de vote par Internet. Il y a finalement renoncé pour les raisons suivantes :

a) Il est difficile d'évaluer les futurs risques émergeant en fonction des lacunes des nouveaux produits.
b) Les risques vont dépendre des enjeux du vote.
c) La nouveauté du système peut tenter un certain nombre de personnes malveillantes à divers titres (par défi, par but de falsification, pour mettre en évidence des lacunes, pour perturber, ...).



2. La sécurité : forces et faiblesses

1. Préambule

Dans son analyse, le Comité a pris en compte divers types de malveillances dont les résultats peuvent se traduire par la perturbation de l'opération, la perte de vote ou la falsification des votes. Le Comité a envisagé divers scénarii dans lesquels une personne malveillante pourrait perturber le bon fonctionnement ou, pire, falsifier les résultats. Il est clairement ressorti des évaluations du Comité que les points faibles sont les éléments hors du contrôle de l'Etat, c'est à dire le poste de travail du votant, d'autres serveurs WEB, le réseau Internet et le votant lui-même.

Pour pouvoir juger du degré de tolérance aux fraudes, le Comité a pris en compte la règle admise par le service des votations pour les opérations électorales actuelles, à savoir que le scrutin est annulé si l'ampleur de la fraude constatée, multipliée par deux, inverse le résultat du vote; reste donc à constater la fraude et à en évaluer l'étendue.

> Le Comité souligne la différence fondamentale qui existe entre une transaction de commerce électronique et le vote par Internet : dans ce dernier, puisque le secret du vote doit être préservé, l'électeur n'a aucun moyen de vérifier que lors du dépouillement c'est bien son vote qui est pris en compte, qu'il n'a pas été effacé, modifié ou ajouté. Dans le cas du commerce électronique, ce contrôle a posteriori existe, il permet de révéler la fraude et éventuellement de la corriger; ce mécanisme de preuve met donc le commerce électronique à l'abri de nombreux doutes quant à sa sécurité.

Il faut aussi noter que dans la situation genevoise, le vote par Internet est une troisième possibilité qui ne remplace pas le système existant à savoir le vote par correspondance, qui est très largement

utilisé (plus de 90%), et le vote "traditionnel" en déposant son bulletin de vote dans l'urne le dimanche matin. Le vote par Internet, ainsi que le vote par correspondance, sont clos le samedi à midi. En cas d'indisponibilité de ces deux derniers modes de vote, l'électeur a toujours la possibilité de déposer son bulletin dans l'urne du local de vote le dimanche matin.

Le vote par Internet peut intéresser les Suisses de l'étranger qui n'ont souvent pas le temps matériel pour renvoyer leur vote par correspondance dans les délais; il reste à espérer que les événements du 11 septembre 2001 n'inciteront pas certains Etats étrangers à proscrire l'utilisation des techniques de chiffrement non triviales.

2. Les mécanismes

Plusieurs mécanismes de sécurité sont mis en œuvre dans toute la chaîne du vote par Internet.

Le protocole SSL

Le protocole SSL supporte l'authentification, la confidentialité et l'intégrité des données échangées entre le poste de travail de l'électeur et le serveur. La solution de chiffrement avec clé de 128 bits a été choisie. L'authentification du serveur est réalisée par un certificat délivré par Verisign. Le mécanisme d'authentification du serveur existe mais le Comité pense que l'électeur n'est ni motivé et ni formé pour effectuer la vérification formelle de ce certificat lors de l'émission de son vote.

Chiffrement à clés asymétriques.

Le suffrage est chiffré dans l'urne électronique par un algorithme à clés asymétriques pour en garantir le secret jusqu'au dépouillement. Deux paires de clés (une paire pour les partis de gauche, l'autre pour les partis de droite) publiques et privées sont générées par WiseKey lors de chaque opération de vote. Les clés privées, permettant le déchiffrement, sont conservées par un officier de police et les mots de passe les activant sont conservés par un notaire jusqu'à la clôture du scrutin.

3. Vulnérabilités

1. Déni de service

Ce type d'attaque vise à saturer le serveur ou un élément du réseau avec un trafic intense pour interdire l'accès en mobilisant toute la bande passante. Ce type d'attaque ne remet pas en cause la validité de l'opération électorale car le vote par Internet n'est qu'une troisième possibilité de voter, analogue au vote par correspondance, donc close le samedi à midi. Comme énoncé ci-dessus la solution de secours consiste à déposer son bulletin de vote dans l'urne du local de vote.

2. Altération du site WEB

Cette malveillance peut prendre deux formes [1]:

- Le point de départ de l'opération est un lien (pointeur URL) situé sur les pages d'accueil du site www.geneve.ch. Si ce pointeur est modifié (piratage), l'électeur pourrait être renvoyé sur un site intermédiaire qui pourrait intercepter son vote.
- Lors d'une opération électorale, plusieurs sites Internet auront des informations sur le thème du vote que ce soit au niveau des partis politiques, des groupes d'intérêt ou d'un simple citoyen. Ces sites, hors du contrôle de l'Etat en ce qui concerne le contenu et la qualité de la sécurité, peuvent être des vecteurs pour déposer un cheval de Troie dans le poste de l'électeur venu s'informer et qui est un candidat potentiel pour un vote par Internet. Plus subtilement, ces sites peuvent proposer un lien pour voter avec un message du genre "Maintenant que vous vous êtes fait une opinion, cliquez ici pour voter"; le seul problème est que le lien peut pointer sur un autre site que le site officiel... Ce mauvais lien a pu être mis volontairement ou par piratage si le site présente un trou de sécurité.

3. Cheval de Troie

Il n'y a aucun contrôle sur le poste de travail de l'utilisateur. Il n'est de loin pas impensable que celui-ci soit contaminé par un cheval de Troie qui falsifie, détourne ou copie le vote.

Un cheval de Troie qui se restreindrait aux votations genevoises peut être introduit dans le poste de travail de l'électeur lors de la visite d'un site WEB ayant pour thème les votations genevoises (l'Etat

[1] Le site http://defaced.alldas.de/ recense plusieurs milliers d'altération de sites.

n'a aucun contrôle sur le contenu des sites WEB autres que les siens) ou lors de la réception d'un mailing électronique ciblant les citoyens genevois.

4. Interception ou détournement de la session

Cette malveillance peut prendre deux formes :

- La liaison a été initialisée correctement mais elle est interceptée sur le réseau entre le poste de travail de l'électeur et le serveur. La liaison entre le poste de l'électeur et l'Etat est une liaison SSL chiffrée avec une clé à 128 bits. Il n'est pas possible d'intercepter cette liaison pour autant que les clés soient bien générées.
- L'électeur s'est connecté à un serveur « malveillant » sans s'en apercevoir, selon un des mécanismes décrits par ailleurs. Avec la malveillance 2 (Altération du site WEB) ou la malveillance 5 (Falsification du serveur de nom) le lien vers le serveur cible est modifié, Le serveur malveillant ouvre de son côté une session vers le serveur de vote mais en modifiant en passant le vote de l'électeur. Le mécanisme des certificats est un outil qui permet à l'utilisateur de vérifier qu'il est sur le bon serveur, mais ceci est au prix d'une manipulation de sa part. La réelle faiblesse de ce mécanisme est que cette démarche de vérification n'est pas une pratique habituelle de l'utilisateur classique de l'Internet. De plus le mécanisme n'est pas bloquant, il fournit simplement un message d'erreur que l'utilisateur peut ignorer pour continuer tout simplement sa transaction.

5. Falsification du serveur de nom (DNS)

Le serveur de nom est le dispositif qui fournit l'adresse IP d'une machine sur le réseau Internet en fonction de son nom. L'action malveillante consiste à modifier un serveur de nom pour qu'il renvoie une adresse IP différente pour le nom de la machine demandée; une telle action malveillante aura pour conséquence d'établir une session avec une machine autre que celle initialement prévue.

N'importe quel administrateur (en titre ou pirate) de serveur de nom, dans une entreprise ou chez un fournisseur d'accès Internet, est en mesure de faire correspondre l'adresse IP de son choix à un nom en le déclarant dans les fichiers de configuration de son serveur de nom.

Une des méthodes de falsification est décrite sous le nom de "DNS cache poisoning".[2]

De plus, sur plusieurs systèmes d'exploitation, dont Windows, cette correspondance nom-adresse IP peut être spécifiée dans le fichier "hosts" du poste de travail de l'électeur. Si une action malveillante ajoute dans ce fichier le nom du serveur de vote avec une autre adresse IP, la session sera déroutée. Lors de l'établissement d'une liaison sécurisée, si le nom du serveur demandé ne correspond pas à celui qui répond, le poste de travail de l'électeur affiche un message d'erreur qui peut être masqué (option du navigateur Internet Explorer).

6. Attaque massive "brute force"

Cette action malveillante consiste à essayer systématiquement tous les codes possibles pour obtenir un « droit de vote ». Le taux de réussite dépend de la bonne répartition de la clé, de sa non-prévisibilité et du taux de transactions du serveur.

7. Facteur humain (ingénierie sociale)

L'électeur qui voudrait utiliser son micro-ordinateur pour voter par Internet n'est généralement pas un spécialiste en informatique. Son équipement est très souvent resté dans l'état où il lui a été fourni, les mises à jour des logiciels, entre autres celles concernant la sécurité, ne sont pas effectuées. [3]

> Il ne faut pas espérer que l'électeur procède naturellement à des manipulations inhabituelles comme la vérification des certificats d'un serveur sécurisé auquel il se connecte.

[2] **DNS Spoofing (Malicious Cache Poisoning),** Doug Sax, November 12, 2000, SANS Institute

[3] **CERT® Advisory CA-2001-20 Continuing Threats to Home Users,** July 23, 2001

Les malveillances exploiteront sa naïveté ou sa candeur comme dans d'autres actions de la vie courante. Que pouvons nous faire, si ce n'est de l'information, pour éviter que l'électeur ne se connecte à un mauvais serveur ou n'utilise un logiciel autre que celui prévu (et éventuellement distribué) par l'Etat?

8. Exploitation de failles

La majorité des attaques sur des systèmes informatiques exploite des failles des systèmes d'exploitation ou des applications. Une technique fréquente consiste à envoyer au système ou à l'application un message plus long que celui normalement attendu. Si le programme de la victime n'a pas prévu cette éventualité, du code malveillant pourra être exécuté.

> Le Comité recommande un suivi régulier et permanent des failles de sécurité découvertes. Dans le cas où elles concerneraient les systèmes mis en œuvre pour le vote par Internet, il conviendra d'appliquer sans délai les corrections de l'éditeur du logiciel en les validant au préalable.

Les mêmes types de failles de sécurité existent sur les postes de travail de l'électeur, hors de portée de l'Etat.

9. Malveillance interne

Il ne faut pas négliger les pressions (terroristes ou hiérarchiques) sur le personnel, ou sa corruption, pour mettre en place un mécanisme permettant la fraude. Bien que peu probable, il n'est pas possible d'exclure cette éventualité à priori.

Par exemple, au niveau de l'application elle-même, une fraude de grande ampleur peut s'envisager avec la participation d'une personne au service de l'Etat participant à l'exploitation du serveur.

Dans un autre exemple, il est possible de "soudoyer" le personnel pour avoir une copie du CD qui sert à imprimer les cartes d'électeurs ou une réimpression sur papier libre des cartes d'électeurs pour disposer des codes d'identification.

10. Complexité et opacité des couches logicielles

L'application s'appuie sur des couches logicielles complexes et opaques qui contiennent des fonctions et services dont la plupart sont inutilisés pour le vote par Internet. Ces fonctions inutiles peuvent être la source de vulnérabilités exploitables. L'amélioration de la sécurité consisterait à réduire au maximum le nombre de couches impliquées, par exemple de s'affranchir de la couche « navigateur » sur le poste de travail de l'électeur. D'autre part, une approche « open source » (ouverture au public du code source) permettrait d'améliorer la crédibilité de l'application, du côté serveur, et à fortiori, du côté votant.

La diversité des postes de travail des électeurs et la complexité des couches de logiciels rend en effet impraticable un audit exhaustif de l'application dans sa forme actuelle.

4. Synthèse des malveillances

Le tableau ci-dessous montre la localisation des vulnérabilités décrites dans ce rapport :

Chez le votant	Infrastructure Internet	Serveur(s) de vote
	(1) Déni de service	
	(2) Altération de sites Web	
(3) Cheval de Troie		
(4) Interception ou détournement de la session		
(5) Falsification des serveurs de noms (DNS)		
		(6) Attaque « brute force »
(7) Facteur humain		
(8) Exploitation de failles		(8) Exploitation de failles
	(9) Malveillance interne	
(10) Complexité des logiciels		(10) Complexité des logiciels

Localisation des vulnérabilités telles que décrites dans ce rapport

Les malveillances envisagées dans cette étude et les possibilités d'action pour en minimiser l'effet sont synthétisées dans le tableau ci-dessous :

Malveillance	Mesure de sécurité envisageable
(1) Déni de service	La solution de secours est le recours au vote dans l'urne le dimanche.
(2) Altérer le site WEB	Développer une procédure pour déployer les correctifs de sécurité. Surveiller régulièrement le serveur
(3) Cheval de Troie	Hors de contrôle de l'Etat
(4) Interception ou détournement de la session	Travailler directement avec des adresses IP dans les liens. Mettre en place une authentification forte du serveur sans action de l'électeur
(5) Falsification du serveur de nom	Se passer du serveur de nom en travaillant directement avec des adresses IP dans les liens
(6) Attaque massive "brute force"	Clés d'authentification correctement générées et bien réparties.
(7) Facteur humain (ingénierie sociale)	Partiellement contrôlable par de l'éducation et de l'information. Distribution du logiciel sur CD-ROM.
(8) Exploitation de failles	Sur le matériel contrôlé par l'Etat : Développer une procédure pour déployer les correctifs de sécurité. Sur le reste : hors de contrôle.
(9) Malveillance interne	Procédures de contrôle interne
(10) Complexité des logiciels	Réduire le nombre de couches utilisées et les remplacer par des logiciels n'ayant que les fonctions nécessaires.

Synthèse des malveillances et des mesures de sécurité correspondantes

5. Intervention contre un serveur malveillant

Si une action malveillante est détectée pendant une opération électorale, les possibilités d'intervention technique rapide sont inexistantes surtout si l'origine (serveur ou personne) est localisée à l'étranger.

Le Comité suggère d'examiner si la législation actuelle permet de lutter efficacement contre des sites diffusant de fausses informations électorales ou étant techniquement dangereux pour la sécurité du vote par Internet.[4]

6. Exigences opérationnelles

Le Comité attire l'attention sur les exigences opérationnelles à respecter pour maintenir le niveau de sécurité d'une application de vote par Internet :

a) Il faut produire un effort de maintenance continu pour suivre l'évolution des lacunes de sécurité des machines, des systèmes et des télécommunications et y apporter les correctifs.

b) Ce suivi suppose un personnel qualifié suffisant.

c) L'ensemble des machines, systèmes et applications impliquées dans le vote par Internet doit avoir une bonne tolérance aux pannes pendant la période de vote. Le Comité propose que l'on évalue les conséquences de la suppression du compte « administrateur système » en cas de panne majeure de l'équipement.

d) L'Etat doit pouvoir intervenir rapidement en cas de malveillance constatée.

e) Pour une meilleure disponibilité, il serait judicieux que les machines soient accessibles via un second fournisseur d'accès à Internet.

3. Les onze principes

1. Les suffrages exprimés électroniquement ne doivent pas pouvoir être interceptés, modifiés ou détournés.

Le point critique de ce principe est le poste de travail de l'utilisateur et l'utilisateur lui-même:

a) Il n'y a aucune protection contre des chevaux de Troie (malveillance 3) qui permettraient d'intercepter, de modifier ou de détourner le vote car l'Etat n'a aucun contrôle sur le contenu du poste de travail de l'électeur.

b) Pour lutter contre le spoofing (connexion sur un faux serveur), **il manque un mécanisme fiable d'authentification du serveur par le votant**. Si du point de vue technique, le certificat permet de vérifier l'authenticité du serveur, il demande une action de la part de l'électeur. Le Comité pense que la culture actuelle de l'utilisateur Internet n'est pas de tester la validité des certificats émis par le serveur, mais plutôt d'ignorer le message du navigateur concernant la sécurité. Le Comité relève qu'il serait préférable de proposer dans la documentation donnée à l'électeur que celui-ci vérifie l'empreinte numérique plutôt que le numéro de série du certificat qui n'est pas un élément de sécurité.

c) D'autre part, la pratique courante de l'utilisateur de base de l'Internet n'est pas d'actualiser les certificats du navigateur. Le Comité pense que l'utilisateur ne se sent pas concerné par l'authentification du serveur.

d) L'adresse du site WEB e-voting est sur le site WEB de l'Etat de Genève. Si par une action malveillante (malveillance 2), on arrive à modifier le lien sur ce site, ce premier principe ne peut pas être satisfait.

e) Pendant l'opération de vote, les données sont en clair sur le poste de travail de l'électeur et sur le serveur pendant un bref instant (voir principe 2).

La session SSL peut être interceptée s'il y a une mauvaise implémentation soit dans le serveur, soit dans le butineur.

[4] A titre d'exemple, le site officiel de l'Organisation Mondiale du Commerce est à l'adresse www.wto.org.. Depuis deux ans, il existe un site pastiche à l'adresse www.gatt.org que l'OMC n'apprécie pas particulièrement ! Signalons également que l'adresse ge-vote.ch, par analogie avec le site officiel ge-vote.geneve.ch, a d'ores et déjà été réservée par un particulier.

Le Comité conseille :

a) de distribuer un CDROM avec les logiciels et les certificats à jour.

b) d'inclure dans le logiciel distribué par CDROM un mécanisme automatique permettant d'authentifier sans ambiguïté le serveur e-voting.

Le CD-ROM peut être réalisé de plusieurs manières, chacune participant à un niveau de sécurité accru :

1. L'approche minimaliste consisterait à distribuer des versions récentes des logiciels standard (navigateurs) et des certificats de sécurité.
2. Il est possible de distribuer des logiciels créés spécialement pour le vote par Internet, afin d'écarter plusieurs vulnérabilités citées dans ce rapport. Ceci est conforme à certains environnements de e-banking actuels.
3. L'option la plus sûre consisterait à ajouter un niveau de sécurité supplémentaire en exigeant que le logiciel sur le CD-ROM ne puisse être exécuté que dans un environnement nettement moins vulnérable que les systèmes d'exploitation grand public; cet effet est obtenu en redémarrant l'ordinateur du votant sur un environnement dédié minimal (soit la véritable réalisation logicielle d'un isoloir, l'*isolware*).

2. Le contenu des suffrages exprimés électroniquement ne doit pas pouvoir être connu par des tiers avant le dépouillement.

C'est le seul point critique de l'application que le Comité a constaté : pendant l'opération de vote les données sont en clair sur le poste de travail de l'électeur et sur le serveur lors du premier échange (sans l'identification de l'électeur), puis lors du deuxième échange (avec l'identification de l'électeur) pendant un bref instant.

En termes techniques : le **vote est en clair quand il passe de la partie externe à la partie interne à confinement accru** du serveur Web sécurisé proposé par HP. Si la partie externe est attaquée par un virus, le certificat n'a aucune utilité.

En effet, la partie externe est (par construction) l'endroit le plus exposé du système. Si quelqu'un arrive à en prendre le contrôle, il peut accomplir à la perfection une attaque "man-in-the-middle" puisqu'il bénéficie du certificat (ou de tout autre mécanisme d'authentification du serveur) et qu'il a tous pouvoirs sur les bulletins qui y passent (puisqu'ils y sont en clair). Tous les mécanismes de sécurité déployés dans les parties intérieures du serveur restent inutiles, et détournement et falsification deviennent un jeu d'enfant.

Afin de préserver la confidentialité du vote, le Comité recommande de prévoir le chiffrement du suffrage sur le poste de travail de l'électeur directement avec les deux clés publiques de l'urne, qui correspondent aux deux clés privées utilisées lors du dépouillement.

De plus, pour éviter que le contenu du suffrage ne puisse être déduit malgré le chiffrement, il faut lui ajouter un champ assez grand dont le contenu est aléatoire, puis chiffrer le tout. Ce point est rappelé ici pour mémoire, car il avait déjà été relevé avant l'analyse de l'application par le Comité.

3. Seules les personnes ayant le droit de vote doivent pouvoir prendre part au scrutin.

Etant donnée la grandeur des clés d'authentification, une attaque massive et distribuée (malveillance 6) n'aurait que peu de chance de succès.

Pour rendre cette probabilité encore plus faible, le Comité propose que l'attribution des clés aux électeurs ne soit pas faite dans l'ordre alphabétique du fichier des votants, mais sur un tri (pseudo)aléatoire.

Le Comité a essayé de voir comment s'approprier les éléments permettant de voter (malveillance 9). Le point critique est la procédure d'impression des cartes d'électeurs qui contient un point faible et humain : il faut "soudoyer" le personnel pour avoir une copie du CD ou une réimpression sur papier libre des cartes d'électeurs. Contrairement au système actuel où un contrôle sur le nombre de cartes d'électeurs permet d'éviter une fraude, pour un vote par Internet il suffit de posséder un élément immatériel (les clés) pour voter. Il faut noter cependant que les éléments ainsi obtenus ne permettent pas directement de voter car il manque la date de naissance, mais une action de "brute force" (malveillance 6) portant seulement sur la date de naissance permet assez vite d'obtenir le droit de vote.

Le Comité été informé que, dans cette application, la base des électeurs n'est pas accessible par Internet, puisqu'elle est sur une machine uniquement raccordée au serveur de vote. Le code NIP est chiffré. Le vol des éléments de vote (clés) depuis Internet ne semble donc pas possible.

Afin de valider qu'il n'y a pas eu création de faux électeurs pendant le transfert dans l'application, le Comité propose de mettre en place une vérification formelle que le nombre d'électeurs inscrits enregistrés dans l'application soit le même que celui de l'Office cantonal de la Population.

4. Chaque électeur ne dispose que d'une voix et ne peut voter qu'une seule fois.

Si l'électeur "repeint" la case à gratter après avoir voté par Internet et qu'il se présente au bureau de vote le dimanche matin, le personnel ne verra pas nécessairement la fraude. Cependant toutes les cartes d'électeurs utilisées dans les locaux de vote sont saisies après le vote pour vérifier s'il y a eu double vote. La fraude serait alors détectée et son ampleur connue. De plus, les fraudeurs seraient passibles de sanctions pénales.

Relevons encore une fois qu'il est très important que l'électeur ne soit pas détourné vers un autre serveur qui (malveillance 4), captant ses éléments d'authentification, voterait à sa place.

5. En aucun cas, même pendant le dépouillement, il ne doit être possible de faire un lien entre un électeur et son suffrage (secret du vote).

Après l'ouverture de l'urne électronique, il serait possible de mettre en corrélation l'heure du vote avec la position du vote dans l'urne électronique.

Pour éviter un lien entre l'électeur et son suffrage par corrélation entre l'heure de vote et la position dans l'urne, le Comité propose un brassage régulier de l'urne électronique.

Le respect de ce principe impose aussi un chiffrement de bout en bout (voir principe 2).

Il faudra évidemment aussi désactiver tout archivage des transactions, notamment dans le serveur Web.

6. Le site doit être en mesure de résister à une attaque en déni de service pouvant aboutir à la saturation du serveur.

Des sondes de mesures seront mises en exploitation pour détecter une attaque de masse.

Il est aussi envisageable de limiter le débit du réseau avant le serveur pour restreindre sur le serveur les conséquences d'une attaque et éviter que celui-ci se mette dans un état imprévisible du fait de la surcharge.

Le serveur www.geneve.ch, point de départ de l'opération de vote, doit aussi être suffisamment robuste pour résister à une attaque.

Si le site devait cependant être bloqué par une attaque en déni de service, il est prévu que les électeurs aillent voter le dimanche dans les bureaux de vote. Pour les électeurs ayant découvert le code permettant de voter par Internet mais ayant été empêché de le faire à cause du blocage, le service des votations autoriserait le vote « manuel » après consultation des informations contenues dans le serveur. Il faut cependant être conscient que, vu la lourdeur de la procédure de contrôle, le nombre d'autorisations qui pourraient être données pendant les deux heures d'ouverture des bureaux de vote sera limité (environ quelques centaines). Il s'ensuit qu'une saturation du site pourrait entraîner une saturation des bureaux de vote.

7. L'électeur doit être protégé contre toute tentative de vol d'identité.

On a vu au principe 3 la faiblesse théorique sur l'impression des cartes d'électeurs.

Une attaque *man-in-the-middle* pourrait être possible, par exemple en modifiant sur le serveur WEB www.geneve.ch le lien vers le serveur e-voting. Les malveillances conduisant à détourner l'électeur vers un autre site visent, entre autres, à "voler l'identité de l'électeur".

8. Le nombre de votes émis doit correspondre au nombre de votes reçus, toute différence doit pouvoir être expliquée et corrigée.

Contrairement à ce que peut laisser entendre l'énoncé de ce principe, il ne peut pas y avoir de correction, mais simplement annulation de la votation si l'erreur constatée modifie le résultat.

Dans l'analyse du Comité, le "vote émis" est pris en compte seulement lorsqu'il arrive sur le serveur de vote. Aucun contrôle n'est possible si l'électeur ne se connecte pas sur le bon serveur. Par analogie avec le vote par correspondance, ce cas correspond au cas où l'électeur envoie son vote à une autre adresse postale que celle du service des votations. [5]

Le Comité a pris connaissance de la description de la transaction de vote et du système transactionnel en place : la transaction est faite par un serveur de base de données renommé, et elle comprend la mise à jour du rôle des électeurs (source du vote, date et heure du vote) et le dépôt du vote dans l'urne électronique (numéro du local de vote, vote chiffré).

L'électeur reçoit quittance que son vote a été enregistré, mais sans confirmation quant à son contenu, secret de vote oblige.

9. La preuve qu'un électeur a voté doit pouvoir être faite.

La violation de ce principe tourne autour de la falsification de la base des votants et elle n'est pas accessible directement par Internet mais seulement par des transactions:

Les 5 PC du service des votations qui enregistrent les votes anticipés sont sur un VLAN. La transaction est chiffrée et l'authentification est assurée par un dispositif de génération automatique de mot de passe dynamique (type Securid).

L'opérateur numérise le code à barre de 12 digits d'identification de l'électeur et reçoit la date de naissance pour vérification.

10. Le système n'accepte pas de vote électronique en dehors de la période d'ouverture du scrutin électronique, lequel système est placé sous l'autorité du Chancelier d'Etat.

Pas de problème sous réserve que les processus automatiques fonctionnent correctement sur les serveurs et que les machines soient bien mises à l'heure

11. Enfin, le bon fonctionnement du système doit pouvoir être vérifié par les autorités désignées à cet effet.

Le Comité suggère :

- qu'un jeu de test établi par les autorités de contrôle soit exécuté avant l'ouverture du vote,
- d'avoir des votes témoins qui passent de manière transparente (puisque chiffré) au travers du système et que l'on doit retrouver (et éliminer) au dépouillement. Par exemple : en créant un local de vote de "test" ouvert pendant l'opération et qui serait utilisé par les "autorités" pour des votes témoins, transparent pour le système de vote électronique, et dont on doit impérativement retrouver, et éliminer, les résultats à la fin de l'opération.
- que le contenu chiffré de l'urne soit publié sur Internet à intervalles de temps réguliers et qu'à la clôture de l'opération les éléments permettant un dépouillement soient rendus publics,

[5] Dans le vote par correspondance la carte d'électeur porte d'un côté l'adresse de l'électeur et de l'autre celle du service des votations. Si l'électeur oublie de retourner la carte lors du renvoi de son vote, il recevra son propre vote à son domicile ! Le service des votations n'a pas de trace de cette erreur.

- que l'on définisse des indicateurs de cohérence en comparant les résultats des trois modes de vote : bureau de vote, correspondance, Internet.
- d'avoir plusieurs copies des bulletins pour une meilleure tolérance aux pannes.

4. Propositions

A l'issue de son analyse, le Comité met en exergue quatre améliorations principales qui contribueront à rehausser la sécurité de l'application de vote par Internet.

1. Chiffrement de bout en bout

Autant pour la crédibilité du système que pour sa sécurité, le Comité propose que les suffrages soient chiffrés sur le poste de travail de l'électeur pour n'être déchiffrés qu'au moment du dépouillement des suffrages.

2. Authentification du serveur

Il a été établi qu'un des points faibles hors du contrôle de l'Etat est que l'électeur se fasse abuser et qu'il se connecte en toute bonne foi sur un autre serveur que celui de l'Etat. Ce serveur intermédiaire pourrait manipuler le suffrage à l'insu de l'électeur. Normalement, le certificat sert à permettre l'authentification du serveur par le poste de travail de l'électeur, mais il demande une manipulation de vérification par l'électeur qui n'est pas naturelle. La solution à ce problème serait que la partie de l'application chez l'électeur effectue automatiquement cette vérification à la place de l'électeur.

3. Distribution du logiciel sur CDROM

Le Comité propose la création d'un CDROM, selon une des trois variantes décrites dans le rapport, afin que l'électeur dispose des certificats à jour et d'un logiciel de vote par Internet qui écarte un maximum de vulnérabilités décrites.

4. Urne de test

Le Comité propose la mise en place d'un mécanisme de test du bon fonctionnement de l'opération de vote par Internet en créant une urne de test à laquelle n'auraient accès que des personnes de confiance telles que les contrôleurs des partis politiques.

Le numéro de cette urne de test serait défini aléatoirement avant le scrutin, de sorte qu'un manipulateur (même interne) malveillant ne sache pas quels sont les suffrages qu'il ne doit pas modifier sous peine que sa fraude soit découverte.

Les suffrages de ces personnes de confiance seraient parallèlement traités à la main et, à l'issue de l'opération électorale, les résultats manuels et par Internet de cette urne devraient concorder.

Les résultats de cette urne étant en réalité des tests, ils ne seraient pas inclus dans le résultat de l'opération électorale.

5. Conclusions

Un Comité sécurité a été mandaté par le Chancelier de la République et Canton de Genève pour évaluer l'application de vote par Internet sous son aspect sécurité en rapport avec onze principes qui doivent être garantis par une opération électorale. A l'issue de son évaluation de l'application, dans son état de développement au 23 septembre, le Comité arrive aux constats suivants :

Niveau de sécurité

Dans la partie de l'application de vote par Internet sous contrôle de l'Etat, les moyens mis en œuvre présentent un bon niveau de sécurité, à l'exception d'une lacune de chiffrement du suffrage. Tout au long de ce rapport, le Comité émet plusieurs propositions pour améliorer encore le niveau de sécurité.

Chiffrement de bout en bout

Pour que le principe 2 (secret du vote) soit garanti dans l'application, il est impératif de corriger la lacune de chiffrement. Le chiffrement du suffrage doit être effectué sur le poste de travail de l'électeur avec les deux clés publiques de chiffrement de l'urne électronique de sorte qu'en aucun cas l'information ne se trouve en clair, même pendant un court instant, avant l'ouverture de l'urne électronique.

La boîte noire

Dans la conception d'une application de vote par Internet, il y a une différence fondamentale à prendre en compte en comparaison à une transaction de commerce électronique: dans le cas du vote par Internet, le secret du vote devant être préservé, l'électeur n'a aucun moyen de vérifier que lors du dépouillement c'est bien son vote qui est pris en compte, qu'il n'a pas été effacé, modifié ou ajouté. Dans le cas du commerce électronique, un contrôle a posteriori existe, il permet de révéler la fraude et éventuellement de la corriger.

Urne de test

Pour tester le bon fonctionnement de l'opération de vote par Internet pendant la période d'ouverture du scrutin, il est proposé de créer une urne de test à laquelle n'auraient accès que des personnes de confiance telles que les contrôleurs des partis politiques.

Législation

Le Comité suggère que l'on étudie en parallèle ce que la législation autorise comme intervention rapide en cas de vulnérabilité constatée pendant une opération électorale et que l'on envisage de la compléter si besoin.

Vote par Internet

Le vote par Internet n'implique pas nécessairement le WEB. Le Comité suggère d'étudier une solution pour le programme du poste de travail de l'électeur qui s'affranchisse au maximum des couches logicielles préexistantes de celui-ci.

Risque difficilement maîtrisable : le poste de travail de l'électeur

Les points faibles difficilement maîtrisables par l'Etat sont le comportement de l'électeur et le contenu de son poste de travail. Comment éviter le détournement ou la falsification du vote entre le poste de travail de l'électeur et l'urne électronique ?

Puisque l'urne électronique est une boîte noire, le Comité pense qu'une **vérification automatique de l'authenticité du serveur** doit être mise en place et qu'il ne faut pas compter sur une action de l'électeur pour effectuer cette vérification. Il faut aussi que l'électeur n'ait pas la possibilité d'utiliser un autre programme que celui distribué par l'Etat pour le vote par Internet. Le risque est en effet que cet autre programme, hostile, connecte le poste de travail de l'électeur, à son insu, à un site Internet intermédiaire qui falsifie son suffrage.

Le Comité est d'avis que l'Etat doit distribuer, sur un support amovible du genre CD-ROM, le programme de vote par Internet, ou en tous cas un noyau de base capable d'établir une liaison sûre et authentifiée et de se mettre à jour automatiquement. L'investissement n'est pas si considérable si on replace ce programme dans un contexte plus général de cyberadministration et pas uniquement vote par Internet.

Annexe : le mandat

REPUBLIQUE ET CANTON DE GENEVE

LE CHANCELIER D'ETAT

Genève, le 23 février 2001

MANDAT SECURITE
Projet vote par Internet
et développement de prestations en ligne

1. Cadre

Dans le cadre du projet "e-voting" visant à mettre en place à l'horizon 2001-2002 un système de vote par Internet en complément au vote traditionnel et au vote par correspondance, la Chancellerie d'Etat souhaite donner un mandat couvrant les aspects liés à la sécurité et permettant de valider les solutions mises en oeuvre.
Ce mandat couvre également le projet relatif au développement des prestations en ligne.

2. Contenu

2.1 Projet de vote par Internet

Le mandataire devra fournir un rapport décrivant les vérifications et contrôles effectués et garantissant que les principes d'un vote sécurisé décrits ci-dessous sont respectés.

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, même pendant le dépouillement, il ne doit être possible de faire un lien entre un électeur et son suffrage (secret du vote).
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.
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, lequel système est placé sous l'autorité du Chancelier d'Etat.
11. Enfin, le bon fonctionnement du système doit pouvoir être vérifié par les autorités désignées à cet effet.

2.2 Développement des prestations en ligne

Le mandat doit aborder les volets suivant :

1. Sécurisation de l'authentification par un système de clé à puce avec code PIN.
2. Sécurisation de l'authentification par un système de carte à puce avec code PIN.
3. Respect de la sphère privée.
4. Respect de la protection des données.
5. Garantie de l'intégrité des données échangées.
6. Garantie de la confidentialité des données échangées.

3. Etendue et délais

3.1 Projet de vote par Internet

Le mandat s'effectuera en deux phases : lors du développement de la solution retenue par le Conseil d'Etat, sur proposition du Chancelier, et lors de son test dans le cadre d'un vote « à blanc ».

S'agissant de la solution retenue, le mandataire étudiera tous les éléments constitutifs et fournira au mandant une première analyse selon les critères ci-dessus

(voir point 2.1). Il s'agit dès ce stade de proposer des mesures correctives éventuelles afin de garantir un niveau de sécurité semblable au dispositif en vigueur.

Dans un second temps, le mandataire étudiera et testera la solution installée et son site lors d'un vote à blanc dont le déroulement est prévu entre juin 2001 et décembre 2001. Sur la base des constats effectués lors du test, il établira son rapport final et ses recommandations en vue de la mise en oeuvre du vote par Internet.

3.2 Développement des prestations en ligne

Les mêmes principes s'appliquent au projet de développement des prestations en ligne. La priorité est cependant donnée quant aux délais au projet de vote par Internet.

Robert HENSLER