

## ANNEXE 1 – Description détaillée du fonctionnement du dispositif

La sécurité du scrutin est un enjeu majeur pour la réussite des élections. Nous présentons ci-dessous notre approche des différentes problématiques et les solutions appliquées.

### SECTION 1.1 - ANONYMAT

#### 1.1.1 L'ANONYMAT LORS DES ECHANGES INTERNET AVEC L'ELECTEUR

Sur la base de la liste électorale consolidée, chaque électeur aura à sa disposition des codes personnels d'authentification uniques.

Ces codes personnels sont générés de façon non prédictible.

Des mesures sont prises pour éviter toute tentative de recherche automatisée des codes personnels de manière frauduleuse (blocage du compte au bout de 3 essais infructueux, catcha...).

Sur le site Internet, le nom et toutes autres informations nominatives, ne sont jamais affichées.

#### 1.1.2 L'ANONYMAT DES VOTES ET LA CONFIDENTIALITE : SEPARATION DES INFORMATIONS NOMINATIVES DU BULLETIN

L'urne recueillant les suffrages et la liste d'émargement sont deux espaces totalement distincts. Il s'agit de deux espaces de stockage sans aucun lien ni relation entre les deux.

Lorsque l'électeur confirme son vote, l'ensemble du traitement est réalisé selon un mécanisme assurant une intégrité parfaite entre la tenue de la liste d'émargement et l'insertion dans l'urne.

De plus, ce traitement garantit l'intégrité du scrutin lors des accès simultanés. Il impose un ordonnancement séquentiel, empêchant, par un exemple, un électeur de voter deux fois simultanément.

#### 1.1.3 LA PRESERVATION DE L'ANONYMAT

Comme indiqué ci-dessus, chaque bulletin inséré dans l'urne ne comprend **aucune** référence (référence nominative ou référence technique) avec l'électeur. Par absence de référence, nous entendons aucun nom, aucune adresse, mais aussi aucun identifiant, ni même aucune empreinte d'un éventuel identifiant qui permettrait, par des traitements croisés ou de jointure, de pouvoir retrouver ultérieurement l'électeur. Le bulletin est **totalement anonyme, même après la clôture**. De plus, lorsque les bulletins sont extraits de l'urne, ils sont mélangés afin d'éviter toute tentative de rapprochement chronologique avec les émargements.

L'anonymat est toujours préservé, même après le dépouillement et l'usage des clés de déchiffrement.

## SECTION 1.II - CONFIDENTIALITE ET CHIFFREMENT

Pour garantir la confidentialité, le prestataire chiffre le bulletin tout au long de son parcours, du poste de travail jusqu'à l'urne, sans aucune interruption. Le bulletin n'est ainsi jamais « déchiffré » sur le serveur applicatif.

Deux niveaux de chiffrement sont mis en place :

- le chiffrement sur le poste de travail, via une implémentation locale en Javascript, est assurée afin de protéger le contenu du suffrage, durant son transport puis durant son stockage dans l'urne jusqu'au dépouillement,
- la totalité des échanges entre le navigateur de l'électeur et le serveur de vote se font selon le protocole HTTPS/TLS ou SSL.

De plus, afin de renforcer la confidentialité, toutes les étapes intermédiaires de construction du bulletin sont réalisées en local sur le poste de l'électeur, sans aucun échange avec le serveur.

Ainsi, le chiffrement du bulletin commence dès que l'utilisateur clique sur le bouton JE VOTE, donc dès son émission. Ces mécanismes garantissent qu'il est impossible de connaître le résultat du scrutin, sans intervention des possesseurs des clés de déchiffrement.

Cette architecture permet de répondre ainsi parfaitement aux exigences de la CNIL sur le chiffrement de bout en bout sans interruption décrite dans sa dernière recommandation n° 2010-371 du 21 octobre 2010.

## SECTION 1.III - INTEGRITE

Par intégrité, il faut entendre : « S'assurer que la saisie faite par le votant sera fidèlement retranscrite lors du dépouillement final ».

L'application assure l'intégrité des votes :

- après avoir exprimé son choix, l'électeur ne peut pas voter à nouveau pour la même élection,
- un électeur ne peut pas voter aux élections auxquelles il n'est pas inscrit,
- une tierce personne, non inscrite, ne peut pas voter.

La solution mise en œuvre est conçue pour garantir :

- aucune altération lors de la saisie du vote Internet, via l'utilisation de HTTPS,

- aucune altération entre la saisie et le dépouillement final, via le chiffrement des bulletins.

#### SECTION 1.IV - DISPONIBILITE

Le service de vote par Internet est accessible 24 heures sur 24 et 7 jours sur 7.

Afin de garantir la meilleure disponibilité, l'ensemble des équipements matériels est redondé.

Le délai de rétablissement du service après une panne est garanti contractuellement par l'hébergeur de la plate-forme.

En fonction des limites définies (nombre de connexions simultanées), le système est capable de surveiller son propre trafic entrant et de le limiter, afin de garantir des temps de réponse optimums et éviter des engorgements.

La disponibilité est mesurée et testée régulièrement pendant toute la période de vote sans perturber et ni altérer la sincérité des suffrages.

Enfin, afin de permettre aux instances de contrôle de surveiller elles-mêmes le bon fonctionnement de bout en bout les traitements applicatifs et cela tout en respectant la plus stricte régularité et sincérité du scrutin, le prestataire met à disposition des comptes ECOLE.

#### SECTION 1.V - AUTHENTIFICATION

Sur la base de la liste électorale consolidée, il est attribué à chaque électeur un identifiant unique, un code d'accès unique et un mot de passe.

Dans le cas où le code d'accès ne peut être fourni par l'entreprise le code d'accès est généré de telle façon qu'il soit impossible de deviner l'identifiant d'une personne, à partir d'un autre identifiant connu.

Le mot de passe est généré de façon aléatoire.

Au niveau de l'authentification sur les services de vote, un mécanisme est mis en place pour éviter de deviner les mots de passe, en bloquant toute tentative de recherches multiples.

Le scellement a pour but de s'assurer de la stabilité dans le temps des différents éléments et dans le cas contraire, de détecter inmanquablement toute modification, quelle qu'en soit la forme ou la justification et avertir les personnes concernées.

Ces différents éléments sont surveillés en comparant leurs empreintes courantes par rapport à un jeu d'empreintes de référence, stocké sur un support stable et non modifiable.

Chaque traitement de surveillance donne lieu à une trace. En cas de différence, une alerte est remontée auprès de la supervision.

Le journal des traitements est associé à l'archive finale réalisée lors de la fermeture du vote.

Il est préconisé qu'un vote test soit réalisé, au préalable, en présence des représentants de commission électorale et éventuellement d'un huissier et/ou d'un expert informatique.

Le test est effectué dans les conditions du réel. La procédure de vote est entièrement déroulée jusqu'au calcul des résultats.

La simulation réalisée sur le site de vote réel passe en revue tous les cas de figure pouvant être rencontrés.

L'objectif est de permettre aux **Bureaux de vote** d'appréhender le fonctionnement global de la solution.