



## **ANNEXE TECHNIQUE**

Description de la solution de vote par internet

# TABLE DES MATIERES

<b>1. CARACTERISTIQUES DE LA SOLUTION</b>	<b>3</b>
1.1. RESPONSIVE WEB DESIGN : 100 % COMPATIBLE SMARTPHONE/TABLETTE	4
1.2. SITE D'ADMINISTRATION DU VOTE	5
1.3. PILOTAGE DU VOTE ELECTRONIQUE PAR LA COMMISSION ELECTORALE	6
<b>2. DESCRIPTION FONCTIONNELLE ET TECHNIQUE DE LA SOLUTION</b>	<b>11</b>
2.1. ETAPE 1 : TRANSMISSION DES CODES CONFIDENTIELS DE VOTE	12
2.2. ETAPE 2 : LE SITE DE VOTE PAR INTERNET	13
2.3. ETAPE 3 : DESCHELLEMENT ET RESULTATS	23
2.4. CONSERVATION, ARCHIVAGE ET DESTRUCTION DES DONNEES	23
2.5. LE JOURNAL ELECTRONIQUE DE L'ELECTION	24
2.6. ARCHITECTURE TECHNIQUE DE LA SOLUTION	25
2.7. SECURISATION DE LA PLATEFORME DE VOTE	28
2.8. NIVEAUX DE SERVICE	30
2.9. CONFORMITE CNIL	31

# 1. CARACTERISTIQUES DE LA SOLUTION

Conformément à vos exigences, PARAGON Elections fournira un site de vote pour les électeurs répondant aux caractéristiques suivantes :

- Un dispositif d'authentification unique de l'électeur sur la base d'un code d'accès et d'un mot de passe uniques générés aléatoirement et complétés **d'un code défi**.
- Au cours de cette procédure, le serveur de vote vérifie que l'électeur est bien autorisé à voter et qu'il n'a pas déjà voté. Dans ce cas seulement, l'électeur accède aux **listes uniquement de son scrutin** dans l'ordre officiellement retenu.
- Les moyens pour l'électeur d'exprimer son suffrage en accédant aux listes des candidats sur une page unique.
- La validation finale du vote après l'affichage du bulletin de vote sélectionné ne se fera qu'après une **double confirmation**, conformément aux recommandations de la CNIL.

Après confirmation du vote par une double validation, la prise en compte et la mémorisation sécurisée et chiffrée de l'expression du vote et de son émargement seront effectives.

L'électeur pourra télécharger et conserver **un accusé de réception à valeur probante** ou demander l'envoi de cet AR par Email après saisie de son adresse Email.

Toutes les informations relatives au vote de l'électeur sont chiffrées par un **algorithme réputé fort**.

La solution garantit à **100% la confidentialité du vote**.

Quelqu'un qui accéderait au poste de l'électeur après son vote n'a pas d'information sur ce vote, ni directement à l'écran (une fois le vote confirmé, l'expression de celui-ci ne peut être retrouvée sur le site), ni via la fonction « retour » du navigateur (la fonction « retour » fait automatiquement revenir à la page d'accueil du site).

Après reconnexion sur le site de vote, l'électeur arrive sur l'accusé de réception sans possibilité de revoter ou de connaître l'expression du vote (ni via les cookies, ni via le cache du navigateur, ni via aucun autre canal).

La solution de vote PARAGON Elections est **compatible** avec tous les principaux navigateurs web sur le marché (Internet Explorer, Mozilla Firefox, Chrome, Safari, Opéra) représentant plus de 97% de compatibilité dans le monde.

Le site de vote est également compatible avec les smartphones et les tablettes disposant des systèmes d'exploitation les plus répandus sur le marché : IOS, Android, Windows XP et ultérieur, Linux.

**Aucun logiciel n'est exigé pour notre solution** qui ne requiert aucun téléchargement, source de faille sécuritaire et trop intrusif.

La solution ne nécessitant aucun logiciel spécifique et étant compatible avec l'extrême majorité des ordinateurs du parc français, l'outil de diagnostic ne paraît pas essentiel, mais nous pourrions cependant mettre en place un contrôle de la version du navigateur web.

## 1.1. RESPONSIVE WEB DESIGN : 100 % COMPATIBLE SMARTPHONE/TABLETTE

Les internautes se connectant de plus en plus souvent depuis leur téléphone ou leur tablette notamment par le flashage d'un QR Code, les sites internet doivent s'adapter aux nouvelles modalités de connexion. Tactilité ou lenteur du débit internet, chaque terminal a des caractéristiques et une résolution d'écran qui lui sont propres et impacte la qualité visuelle du site de base.

L'approche technologique de création d'un site internet doit être repensée pour mieux anticiper les différentes contraintes liées à chaque support. Le **Responsive Web Design** est aujourd'hui une solution incontournable quel que soit le support de navigation emprunté.

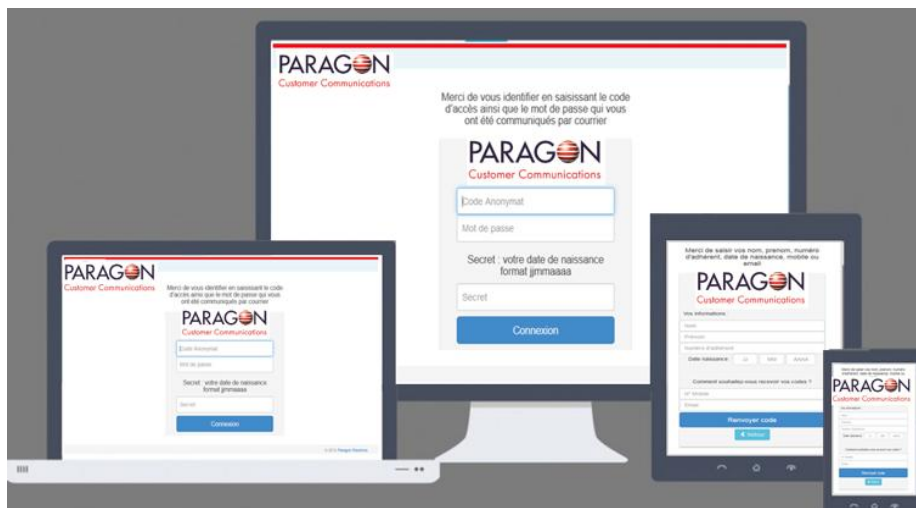
Les avantages du Responsive Web Design sont nombreux :

- plus de réactivité au site web qui s'adapte alors aux différentes résolutions d'écrans disponibles.
- universaliser l'affichage d'un site web en utilisant les nouvelles règles acceptées par la grande majorité des navigateurs.
- Les colonnes et les images s'ajustent, se redimensionnent et se déplacent automatiquement selon que la résolution d'écran l'exige.
- ergonomie optimale en sauvegardant intacte la qualité de l'information du site de vote.

Avec le **Responsive Web Design**, c'est l'assurance d'une **URL unique, peu importe le terminal utilisé (mobile ou fixe)**. En effet, le non-ajustement du site au support de navigation peut affecter grandement l'expérience de vote en ligne pour l'électeur.

Le site s'affiche automatiquement en fonction de l'écran sans demander de quelle manière l'utilisateur souhaite naviguer.

La plateforme de vote par Internet PARAGON Elections est un site internet Responsive Web Design, totalement compatible avec les Smartphones et Tablettes



## 1.2. SITE D'ADMINISTRATION DU VOTE

---

Conformément à vos exigences, PARAGON Elections fournira un site d'administration pour le bureau de vote et l'ensemble des personnes habilitées :

- Chaque personne désignée aura en sa possession un code et un mot de passe pour se connecter au **site d'administration**.
- Le site de gestion/administration permettra le **scellement** puis le **descellement** de l'élection.
- La possibilité de générer des clés de scellement ou la possibilité au bureau de vote de saisir leurs clés de scellement : **Ces clés sont personnelles et connues seulement** des membres les saisissant.
- Le **dépouillement/déchiffrement** des expressions de vote (bulletins de vote électroniques)
- La **génération des résultats** de l'élection par scrutin (urne) dans un fichier non modifiable et horodaté.
- **Les listes d'émargement** et l'accès au taux de participation tout au long du scrutin et après descellement/dépouillement. Plusieurs **niveaux du taux de participation** sont paramétrés : global, par scrutin, etc...
- Le suivi en temps réel des **alertes techniques et applicatives** et les interventions éventuelles sur la solution de vote après le scellement dans un journal des interventions sécurisé, non modifiable et accessible uniquement par les seules personnes habilitées.
- La **garantie** que la version applicative et technique ainsi que les données (fichiers des électeurs, expression des votes et caractéristiques des scrutins) **n'ont pas été altérées**. Cette garantie est contrôlée par des **prises d'empreintes** régulières, aléatoires et déclenchées manuellement par les personnes habilitées quand ils le souhaitent permettant un suivi précis de la non-modification des données tout au long de la période de vote.
- Les dates et heures d'ouverture et de fermeture sont mentionnées avant le scellement et paramétrable avant le processus de scellement selon les souhaits du client. Aucun vote ne pourra être enregistré avant et après ces dates. Avant l'ouverture et après la fermeture, un message avertira l'électeur que l'élection n'a pas encore commencée ou que l'élection est terminée.
- **Aucun accès à des résultats partiels** ne sera possible. Seule la participation sera consultable par les personnes habilitées (gestionnaire, commission électorale, expert)

### 1.3. PILOTAGE DU VOTE ELECTRONIQUE PAR LA COMMISSION ELECTORALE

Le bureau de vote (ou commission électorale) a un rôle de surveillance du scrutin et doit disposer des outils nécessaires pour s'assurer de la bonne mise en œuvre de la plateforme de vote électronique. La CNIL précise aussi que le bureau de vote doit pouvoir agir sur le déroulement du scrutin en cas d'anomalie constatée.

A ce titre elle sera formée et elle dispose de codes d'accès spécifiques à l'interface gestionnaire lui permettant de :

- Procéder au scellement/descellement des urnes électroniques.
- Suivre le taux de participation en temps réel des scrutins en cours de vote

La participation globale et son évolution graphique dans le temps affichée à la demande après connexion offrira des indicateurs précis et en temps réel. La participation pourra également être observée par scrutin pour évaluer les scrutins à plus forte ou à plus faible participation. A la fin du vote internet, ces taux de participation seront historisés.

The screenshot shows a web interface titled "DEMONSTRATION CSE". At the top, there is a navigation menu with the following items: "Menu", "Accueil", "Participation", "État scellement", "Journaux", "Sceller / Desceller", "Résultats", "Mettre en pause", and a "Déconnexion" button on the right. The main content area contains six colored buttons arranged in a 2x3 grid:

- Participation** (teal): Suivre les taux de participation de vos élections
- État scellement** (teal): Savoir dans quel état sont les urnes
- Journaux** (yellow): Consulter les historiques de vos élections
- Sceller / Desceller** (red): Sceller et desceller vos urnes
- Résultats** (green): Consulter les résultats de vos élections
- Mettre en pause** (yellow): Mettre en pause une ou plusieurs élections

Taux de participation global		
Nombre d'électeurs	Nombre de votants	Résultat
2000	0	0 %

Taux de participation global par scrutin				
Libellé du scrutin	Nombre d'électeurs	Nombre de bulletins	Résultat	Liste émargement
ELECTION CSE TITULAIRE AGENTS DE MAITRISE	500	0	0 %	<a href="#">Voir</a>
ELECTION CSE TITULAIRE CADRES	500	0	0 %	<a href="#">Voir</a>
ELECTION CSE TITULAIRE EMPLOYES	1000	0	0 %	<a href="#">Voir</a>
ELECTION CSE SUPPLEANT AGENTS DE MAITRISE	500	0	0 %	<a href="#">Voir</a>
ELECTION CSE SUPPLEANT CADRES	500	0	0 %	<a href="#">Voir</a>
ELECTION CSE SUPPLEANT EMPLOYES	1000	0	0 %	<a href="#">Voir</a>

[Télécharger le récapitulatif d'émargement](#)      [Télécharger les listes d'émargement](#)

[Retour à l'accueil](#)

### 1.3.1. MISE EN PAUSE DU SCRUTIN

Mettre en pause le scrutin (par les membres du bureau de vote) si une irrégularité est constatée (recommandation CNIL).

Libellé de l'élection	État	Action
ELECTION CSE TITULAIRE AGENTS DE MAITRISE	en cours	<a href="#">Mettre en pause</a>
ELECTION CSE TITULAIRE CADRES	en pause	<a href="#">Reprendre</a>
ELECTION CSE TITULAIRE EMPLOYES	en cours	<a href="#">Mettre en pause</a>
ELECTION CSE SUPPLEANT AGENTS DE MAITRISE	en cours	<a href="#">Mettre en pause</a>
ELECTION CSE SUPPLEANT CADRES	en cours	<a href="#">Mettre en pause</a>
ELECTION CSE SUPPLEANT EMPLOYES	en cours	<a href="#">Mettre en pause</a>

[Retour à l'accueil](#)

Choisissez le premier scrutin pour lequel vous souhaitez voter. À la fin de votre premier vote, vous pourrez renouveler l'opération pour les scrutins suivants jusqu'à épuisement de tous vos scrutins.

<b>ELECTION CSE TITULAIRE CADRES</b>
Election du <b>07/01/2019 15:00:00</b> au <b>07/01/2019 15:15:00</b> (Heure de Paris) <a href="#">L'élection est en pause.</a>
<b>ELECTION CSE SUPPLEANT CADRES</b>
Election du <b>07/01/2019 15:00:00</b> au <b>07/01/2019 15:15:00</b> (Heure de Paris) <a href="#">Choisir ce scrutin</a>

### 1.3.2. CONTROLE D'INTEGRITE DU SCRUTIN

Contrôler l'intégrité du scrutin en déclenchant une prise d'empreinte de la solution. Cette action permet de s'assurer que rien n'a été modifié en cours de vote (par conception logicielle, rien ne peut être modifié, mais il doit être prévu un moyen pour le bureau de vote de le vérifier).

Ces prises d'empreinte peuvent être déclenchées manuellement par un membre du bureau de vote, et elles sont également réalisées par la plateforme de vote elle-même de manière régulière et aléatoire afin de détecter la moindre anomalie en temps réel.

#### Intégrité du scellement

[Télécharger le pdf](#) [Déclencher un test](#)

Date	Type	Empreinte	Statut	Site
Le 2019-01-07 à 15:14:40	Manuel	1001233981	OK	Principal
Le 2019-01-07 à 15:14:42	Manuel	1001233981	OK	Principal
Le 2019-01-07 à 15:14:46	Manuel	1001233981	OK	Principal

[Retour à l'accueil](#)

### 1.3.3. SUIVI EN TEMPS REEL

Le suivi en temps réel des alertes techniques, applicatives et les interventions éventuelles sur la solution de vote après le scellement dans un journal des interventions sécurisé, non modifiable et accessible uniquement par les seules personnes habilitées.

Journal [Sceller / Desceller](#) [Résultats](#) [Mettre en pause](#)

## DEMONSTRATION CSE

### ELECTION CSE TITULAIRE CADRES

Date	Libellé	Commentaires
le 07/01/2019 à 15:02:18	Validation	Validation des informations avant scellement
le 07/01/2019 à 15:04:36	Scellement	Scellement de l'élection via le groupement SCELLEMENT
le 07/01/2019 à 15:12:10	Interruption	Interruption du scrutin
le 07/01/2019 à 15:13:47	Interruption	Reprise du scrutin

[Retour à la liste des élections](#)

### 1.3.4. SCELLEMENT DU SYSTEME

---

Avant de procéder au vote, il faudra sceller l'élection. Le client détermine l'heure d'ouverture et de fermeture du scrutin qui conditionne la période de vote par internet puis scelle l'élection en saisissant les clés de chiffrement distinctes

Le processus de **scellement** consiste à réaliser les opérations suivantes :

- le scrutin ne peut pas être ouvert tant que l'opération de scellement n'a pas été réalisée
- le scellement est effectué par le bureau de vote via des clés privées qu'il demeure le seul à connaître. La saisie de cette clé (pour rappel toutes les connexions sont réalisées en https) permet de **générer un certificat dont la clé publique est seule communiquée et enregistrée par la plateforme** pour le chiffrement des expressions de vote, conformément à la CNIL.
- le **scellement déclenche le calcul d'une signature des programmes applicatifs** aussi bien pour le site web (développé en php) que pour l'application serveur (développé en java). Le programme lui-même qui effectue le calcul de signature est intégré au calcul de signature si bien qu'il ne peut être altéré sans modification de la signature.
- Durant le scrutin il est possible à tout moment de consulter par les membres des bureaux de vote et le gestionnaire client le journal électronique de l'élection pour **vérifier que les signatures** des fichiers électeurs, candidats, ainsi que des programmes applicatifs sont inchangées et ainsi garantir la **stabilité et l'intégrité** de la plateforme de vote.

L'opération de scellement **déclenche** automatiquement les opérations suivantes :

- **impossibilité de modifier** toute donnée relative à l'élection : ajout ou modification de données électeur (nom, adresse, identifiant, catégorie,...), ajout ou modification de données candidat et/ou liste de candidature (nom de liste, nom et prénom de candidat, profession de foi,...),
- suppression de toutes les expressions de vote antérieurement enregistrées dans l'urne notamment pour les opérations de tests et de recette.
- **effacement de toute information associée aux listes d'émargement**, c'est-à-dire l'effacement de toute information de date et heure de votes tests, accusé de réception existant dans la base avant le scellement.

**Conformément aux dernières recommandations de la CNIL le prestataire n'a pas connaissance des clés de scellement** : seuls les acteurs du scellement (habituellement les membres des bureaux de vote) en ont connaissance. La plate-forme de vote ne doit donc pas les générer pour eux.

Objectif 1-08 de la CNIL :

*Renforcer la confidentialité et l'intégrité des données en répartissant le secret permettant le dépouillement exclusivement au sein du bureau électoral et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé.*

Nous proposons une solution dont le nombre de clés de scellement est paramétrable avec les principes suivants :

- La génération des clés de scellement est prévue avec la saisie de clés de scellement par les membres de la commission électorale lors de la cérémonie de scellement complétée de la génération de clés de secours remis à des autorités tierces de confiance.
- Les clés de secours seules ne permettent pas le descellement de l'élection.
- Chaque clé de scellement saisie dans l'interface lors de la cérémonie de scellement permet de chiffrer un fragment de la clé globale de scellement et seules les personnes ayant saisie leur clé pourront procéder au descellement du fragment concerné
- Les clés saisies par les membres de la commission électorale devront être réputée forte. 8 caractères (ce nombre peut être porté à 12 pour des élections très sensibles) contenant à minima une majuscule, une minuscule, un chiffre et un caractère spécial.
- Le descellement de l'élection ne peut s'effectuer qu'avec la saisie du nombre de clés défini par le seuil minimum de clés, pouvant inclure les clés de secours confiées à des tiers de confiance sans que ceux-ci soient suffisants pour pouvoir desceller l'élection.

Pour rappel, la CNIL impose la saisie de 3 clés minimum au scellement et le déscellement par 2 au moins des 3 clés. Ce nombre de clés est paramétrable.

Principes du scellement/descellement :

- Pour effectuer le contrôle de conformité des clés de scellement lors du descellement, les identifiants des personnes ayant effectué le scellement sont concaténés et chiffrés avec la clé privée, puis une empreinte est générée et mémorisée par le serveur pour comparaison lors du descellement.
- La validation de la saisie des clés de scellement déclenche également la génération d'une empreinte des fichiers électeurs, candidats ainsi que des programmes exécutables du serveur et du site Internet qui sont déposés dans le CFE Paragon.
- De manière aléatoire, des empreintes du fichier des électeurs, des candidats et programmes exécutables sont réalisées de manière aléatoire à l'initiative du serveur ou à l'initiative du client sur son interface de gestion selon le même procédé que lors du scellement. Ces empreintes sont déposées sur le CFE Paragon avec toutes les fonctions associées (horodatage et garantie d'intégrité) tout en enregistrant l'opération sur le journal d'horodatage les éléments de la preuve de dépôt au CFE Paragon. Au terme de l'élection, après descellement un contrôle de similitudes des empreintes déposées est effectué et généré en liaison avec le journal d'horodatage.
- Un contrôle de validité de la saisie des clés, et donc de la clé globale de déchiffrement est immédiatement effectué en procédant à la comparaison du résultat du calcul de l'empreinte des identifiants des personnes ayant effectué le scellement chiffré avec la clé privée qui vient d'être déchiffrée, par rapport à l'empreinte générée lors du scellement. En cas de discordance, la saisie de la clé de scellement n'est pas validée.
- Après validation du descellement, l'ensemble des bulletins déposés dans l'urne électronique sont déchiffrés pour dépouillement et calcul des résultats.
- Après descellement, l'ensemble des informations sont accessibles : liste d'émargement, urne, résultats,...

Scellement / Desceller Résultats Mettre en pause

### DEMONSTRATION

#### SCELLEMENT

##### Scellement du groupement

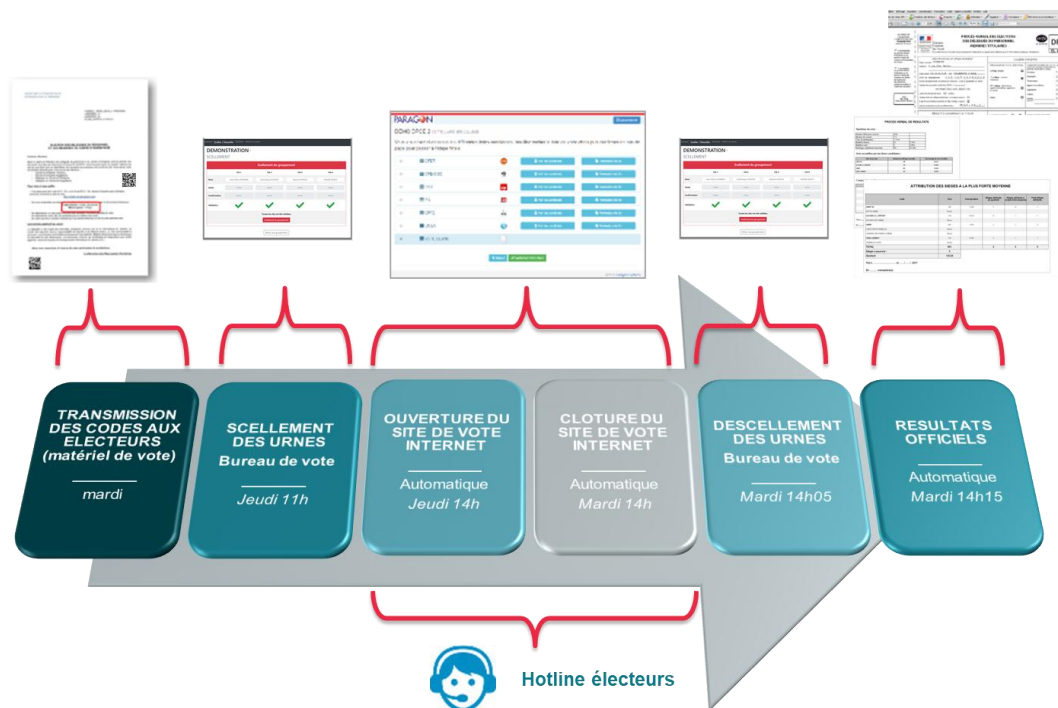
	Clé 1	Clé 2	Clé 3	Clé 4
Nom	Jean-Pierre DURAND	Dominique DUPONT	Maurice DUPUIS	Mireille DUPUY
Saisie	*****	*****	*****	*****
Confirmation	*****	*****	*****	*****
Validation	✓	✓	✓	✓

Toutes les clés ont été validées.

Scellement du groupement

Retour aux groupements

## 2. DESCRIPTION FONCTIONNELLE ET TECHNIQUE DE LA SOLUTION



Les heures d'ouverture et de fermeture du scrutin sont fixées par le Client. Ce paramètre fera partie des éléments protégés par le scellement de l'opération de vote et ne seront plus modifiables après le scellement de la plateforme réalisé.

L'électeur recevra, par Courrier et/ou Email, les éléments pour savoir comment procéder le jour du vote (note explicative, code d'accès, ...).

Chaque électeur disposera d'un **code d'accès unique** (aussi appelé login) et d'un **mot de passe**, générés aléatoirement et dont l'**unicité** est contrôlée à l'import des fichiers électeurs et candidats et à l'export avant l'édition des courriers. L'électeur se connecte en saisissant son code d'accès, son mot de passe et un **code défi** (cette information devra être fiable et connue de l'électeur lui-même). Nous recommandons d'utiliser comme code défi une donnée chiffrée pour une saisie facilitée.

Le vote validé, entraînera plusieurs actions :

- émargement avec génération de l'accusé de réception
- alimentation du taux de participation
- chiffrage du bulletin de vote sur le poste de l'électeur
- dépôt du bulletin de vote chiffré dans l'urne chiffrée en empêchant tout recouplement entre l'heure de dépôt de l'expression de vote et l'heure d'émargement ce qui garantit l'anonymat d'une façon optimale.
- enregistrement du vote qui déclenche l'impossibilité d'une nouvelle expression de vote par le même électeur pour l'élection considérée

Ces opérations reposent sur une gestion en temps réel des données directement sur les bases de données de l'élection.

Le site internet de vote ne nécessite aucune installation de logiciel sur le poste de l'utilisateur, l'installation de « JAVA » n'est pas requise. Le site de vote dispose d'un certificat HTTPS de niveau A compatible avec les normes RGS et ETSI TS 102 042 permettant des échanges totalement sécurisés entre le serveur et le client.

L'ensemble du processus de vote comprend le scellement, le vote par internet, le dépouillement des urnes électroniques, le descellement et le calcul des résultats.

## 2.1. ETAPE 1 : TRANSMISSION DES CODES CONFIDENTIELS DE VOTE

Pour chaque électeur, il y a 2 codes confidentiels à transmettre : 1 code d'accès + 1 mot de passe.

L'électeur devra saisir ces 2 données pour se connecter au site de vote et procéder au vote électronique. Il est possible de lui demander de saisir une 3<sup>ème</sup> donnée, par exemple son matricule.

L'envoi du code d'accès est prévu par e-mail à l'adresse de l'électeur.

### Exemple d'e-mail d'envoi du code d'accès :

À ce message se réfère le cas échéant à :



**VOUS CODES D'ACCÈS POUR VOUS IDENTIFIER :**

Bonjour Mme Cythia Palazzo,

Dans le cadre du renouvellement de la représentation de ses membres participants, la Mutuelle Saint-Martin organise les élections des délégués.

Ces élections constituent un moment important de la vie démocratique de notre mutuelle : elles permettent à chaque adhérent de participer activement aux décisions et à l'orientation de notre organisation.

Dans le cadre de sa stratégie RSC et afin d'élargir l'exercice démocratique au plus grand nombre, ces élections se dérouleront de façon dématérialisée. A cet effet, vous êtes invité(e) à voter en ligne via notre plateforme sécurisée.

Le vote se déroulera, du **lundi 1er décembre 2025 à 08h01** (heure Métropole) **jusqu'au vendredi 12 janvier 2026 à 23h59** (heure Métropole).

Pour vous identifier sur votre espace de vote en ligne, ci-dessous vos **codes d'accès personnels et confidentiels** :

**Code d'accès : 1234567890**

**COMMENT VOTER ?**

**1. Cliquez sur le lien ci-dessous ou saisissez l'adresse internet du site de vote dans la barre d'adresse de votre navigateur :**

[mutuelle.saintmartin.simplivote.fr?no=1](mailto:mutuelle.saintmartin.simplivote.fr?no=1)

Prévisualisez le navigateur internet depuis l'adresse : Mutuelle Saint-Martin (SimpliVote) dans une dernière session et sans passer par un navigateur sécurisé.

**2. Identifiez-vous** en renseignant votre code d'accès indiqué ci-dessus, ainsi que votre mot de passe temporaire,

à vous sera fourni votre code d'accès cliqué sur le lien « [Maux codes privés vos codes](#) » présent sur la page d'accueil du site de vote.

**3. Décrivez votre mot de passe personnel et accédez à votre espace de vote,**

**4. Sélectionnez** les candidats qui se présentent à la fonction ou le vote blanc,

**5. Puis, validez** votre bulletin de vote.

N'oubliez pas de vous déconnecter à l'issue de votre participation.

Le site de vote est accessible sur tout type de terminal (ordinateur, smartphone et tablette), 24 heures sur 24 et 7 jours sur 7, à partir d'une simple connexion Internet.

Si vous rencontrez des difficultés techniques, vous pouvez contacter l'assistance téléphonique au **09 72 30 55 03**, 24 heures sur 24 et 7 jours sur 7.

Votre participation est essentielle pour garantir une représentation fidèle et dynamique des adhérents au sein de la mutuelle.

Nous vous remercions de votre engagement et de votre confiance.

Le Conseil d'Administration de la Mutuelle Saint-Martin

Vos données personnelles sont destinées strictement en vue de la Mutuelle Saint-Martin ainsi qu'à ses prestataires participant à la gestion de votre contrat. Elles sont collectées pendant toute la durée de votre contrat et sont traitées en toute sécurité par les lieux applicables de la loi applicable. À ce titre, les données collectées sont obligatoirement passées par un prestataire de votre choix. Vous pouvez exercer vos droits de la loi applicable et librement modifier de la personne (RFS) sans disposer d'un droit d'accès, de modification, d'effacement, de limitation d'opposition et de la possibilité de vos données à caractère personnel, ainsi que du droit d'opposition des données ou le droit de vos données personnelles après votre décès. Pour l'exercice de ces droits, contactez votre ou l'organisme de la Fédération des Associations de la Mutuelle Saint-Martin, 7 rue Dauphine-Tourne-7, 201 Paris cedex 05 - [direction@mutuelle-saintmartin.fr](mailto:direction@mutuelle-saintmartin.fr).

Vous reconnaissez totalement votre identité et l'exactitude des données que le site de vote de votre organisme (SimpliVote) a recueillies et accepte les conditions de la LSI en matière de sécurité et de confidentialité, en particulier la certification LSI n° 2019-011 du 27 avril 2019 portant adoption d'une norme française relative à la sécurité des systèmes de traitement automatisés de données, notamment via Internet.

Cherchez le nom de vos élections, et nous consulter pour toute information complémentaire, cliquez [ici](#).

## 2.2. ETAPE 2 : LE SITE DE VOTE PAR INTERNET

### 1. Authentification

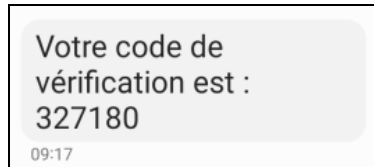
- L'URL sera définie à votre convenance, par exemple : <https://smeno.simplivote.fr>
- Le logo et les textes sont paramétrables
- La communication entre le terminal de vote de l'électeur et les serveurs de vote est en HTTPS (SSL de niveau A).
- Le code d'accès (identifiant) de l'électeur sera généré par Paragon de manière aléatoire. Ce code est anonyme et sera unique sur 10 positions numériques.
- Le mot de passe sera défini directement par l'électeur (voir processus ci-dessous)
- Le système bannit un électeur (comme un fail2ban) qui se trompe 5 fois de mot de passe avec un code d'accès valide, ceci afin de bloquer les éventuelles « attaques en masse » (cette donnée est paramétrable).
- Pour se connecter, l'électeur doit saisir son code d'accès reçu par e-mail et la réponse à la question secrète (son numéro de matricule dans l'exemple ci-dessous)

The screenshot shows the login interface for the 'ELECTION CSE 2026' on the Deloitte website. It features a 'Code d'accès' field, a 'Matricule' field, and a 'Connexion' button. A countdown timer shows 173 days, 18 hours, 55 minutes, and 19 seconds remaining. The page also includes a footer with links for 'ESPACE DE TEST', 'FAQ', 'ASSISTANCE TECHNIQUE', and 'MENTIONS LÉGALES'.

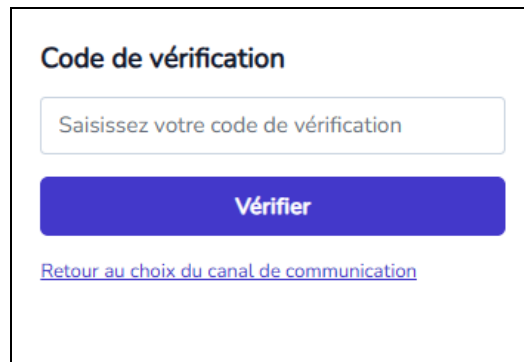
- Après avoir cliqué sur le bouton « Connexion », l'électeur est invité à cliquer sur le bouton « Envoyer » pour recevoir un code de vérification par sms.

The screenshot shows a form titled 'Envoyer le code de vérification'. It has a radio button selected for 'Par SMS' and a text input field containing the number '0601020304'. Below the input field is a blue 'Envoyer' button.

- Réception du code de vérification par sms



- Saisie du code de vérification



**Code de vérification**

Saisissez votre code de vérification

**Vérier**

[Retour au choix du canal de communication](#)

- Après avoir saisi le code de vérification, l'électeur est invité à définir son propre mot de passe personnel et confidentiel de vote (mot de passe définitif)



**Changer votre mot de passe**

**Nouveau mot de passe**

Saisissez votre nouveau mot de passe

**Confirmation de votre nouveau mot de passe**

Saisissez à nouveau votre mot de passe

**Modifier**

- Une fois son mot de passe enregistré, l'électeur est automatiquement redirigé vers son espace de vote sécurisé (voir § Présentation des scrutins)

## 2. Présentation des scrutins (accessible AVANT et PENDANT le vote)

- L'électeur visualise tous les scrutins accessibles sur la même page
- L'électeur choisi le scrutin pour lequel il souhaite voter en premier

**Deloitte.** ELECTION CSE 2026

### Liste des scrutins

**Election CSE 2026**  
Election du 9 juin 2026 à 8h au 15 juin 2026 à 16h (heure de Paris)

Collège 1 - Scrutin Titulaires [Choisir ce scrutin >](#)

Collège 1 - Scrutin Suppléants [Choisir ce scrutin >](#)

ESPACE DE TEST      FAQ      ASSISTANCE TECHNIQUE      MENTIONS LÉGALES

- Les scrutins pour lesquels il n'a pas encore voté sont clairement identifiés s'il a déjà participé à d'autres scrutins

**Deloitte.** ELECTION CSE 2026

### Liste des scrutins

**Election CSE 2026**  
Election du 9 juin 2026 à 8h au 15 juin 2026 à 16h (heure de Paris)

Collège 1 - Scrutin Titulaires  
Vote enregistré le mercredi 17 décembre 2025 à 12h15  
Accusé de réception  
n°6ad853c68bfd4c5831d251d9c1b9a5cf4e2d62dec15cee675a3415e47639cfee [Voir l'accusé de réception >](#)

Collège 1 - Scrutin Suppléants [Choisir ce scrutin >](#)

ESPACE DE TEST      FAQ      ASSISTANCE TECHNIQUE      MENTIONS LÉGALES

### 3. Présentation des listes de candidats (accessible AVANT et PENDANT le vote)

- L'électeur visualise toutes les listes de candidats sur la même page.
- L'électeur peut consulter les candidats de chaque liste en cliquant sur le bouton « Voir les candidats » ainsi que la profession de foi associée en cliquant sur le bouton « Voir la profession de foi »

**Deloitte.** ELECTION CSE 2026

## Listes candidates

Vous visualisez ci-dessous les différentes listes candidates.

Vous pouvez consulter les professions de foi en cliquant sur le bouton "Voir la profession de foi".

Pour sélectionner la liste de votre choix, cliquez sur le bouton "Choisir cette liste", sinon cliquez sur le bouton "Je vote blanc".

### Collège 1 - Scrutin Titulaires

- Cfdt:** Liste CFDT  
Voir les candidats | Voir la profession de foi | Choisir cette liste
- CFE CGC:** Liste CFE-CGC  
Voir les candidats | Voir la profession de foi | Choisir cette liste
- cgt:** Liste CGT  
Voir les candidats | Voir la profession de foi | Choisir cette liste
- UNSA:** Liste UNSA  
Voir les candidats | Voir la profession de foi | Choisir cette liste

VOTE BLANC  
Je vote blanc

< Retour

**Cfdt:** Liste CFDT

- Monsieur Ahyyyyy AMXXXXX
- Madame Hyyyyyy AKXXXXX
- Monsieur Edyyyyy ROXXXXX

#### Profession de foi

scriptorem delicatissimi duo ad. Error decore  
maquiam in vis.

in hac modo nibh cita, dita graeco  
voluptatum sit no. An duo vitae melius  
ceteros, omnis accusam convenire eam cu,  
pro ut tota adhuc persecuti. Ex sed unum  
utroque albucius, ullum aperirian expetenda no  
cum. De omnitan eligendi aliquando pri, ut sea  
meliore offendit corrupti, cum ad oratio  
ventus. Ea vis wisi autem malorum, doming  
melius delent ea eos, ignota inductum sea te.  
No labores civibus honestatis vel, ex vis fugit  
vocent aliquando, nisi commune sententiae ei  
eos.

An ullum ultricies cotidieque pri, ei vel  
utinam nominati prodesset. Commodio  
principes sea in, sumo laudem voluptaria ut  
quo. Ea duo brute illum aeterno, mea ei nisi  
alio epicuri. Ea sea diareet iucillus, delent  
faciliss splendide sed no, reque aperirian  
insolens quo id. Ut his idique iuvaret, ei vis  
salutandi necessitatibus, nam veritus  
complectitur an. Ut iuvaret detracto qualique  
vel, in falli veniam inimicus nam.

Malis ceteros in nam, et discere meliore ex.  
Vizae tibique intellegam te sit, laoreet  
petentium occurreret cum no. Eam no reque  
blandit expetenda, pertinax expetenda et mel.  
At vis fastidi atororum perpetua, mea feugiat  
doceendi ad, tempor venar ea mei. Admodum  
nominavi duo ei, cu vel utroque  
consequuntur.

Ad mea quas voluptatibus, mei id possim  
iudicabit disputationi, discere dolorum  
periculis mel at. Eos ei inani nostrud scripserit,  
est concepitam eloquentiam comprehensam  
ut, ex est putent meliore. Ut est elit laudem  
queque, nam dico pertinax sadipiscing te.  
Per meis takinata adolescens ad, ilisque  
mediocrem intellegam vix no. Mea omnis  
iudus ex nec, tincidunt omitterant no sit. Ad  
ius autem corrupti coos

>Lorem ipsum ei iusto utamur prompta eam,  
cum sonet graecis definitibus cu. Eos eu  
nusquam molestiae, eos porro etiam graecis  
in, id eam elefendit definitones. Per ex debet  
perfecto itacunda, tempor sententiae  
adipiscing eos no, meliore nostrum via te. Cu  
aliquando liberavisse vel, est nulla dolore ne,  
eam id nisi minim putant. Cu viderer veritus  
mel, dita labore timeam te nec, duis quaque  
detracti duo ad.

Iudicio suscipiantur ad sed, et pri dita soluta,  
ne sed quem illud neglegentur. Menandi  
recusabo accusamus ea vel, ex vix omnium  
labores sensibus, facilis conclusionemque has  
at. At vix facete possim inductum, mel id  
illum oblique instructor, usu no magna  
venar suscipit. Duo no accusam periculis  
similique. Te suas fabellas voluptatum ius,  
choro expetenda vituperata nec te. Cu  
utroque salutandi nam, per iudus ornatus  
verterem id, simul habemus patrioque pri ad.

Nemore caeuae intellegam nam ne, mutat  
voluptua mondomus et qui, usu diam ferri ut.  
Ea dictas periculo maluisse nam, iusto ridens  
occumsum per ea. Eum altera blandit periculis  
id, vivendo pertinax duo ei, ut ius elit quaerito  
euripidis. Erat sanctus facilis num in, id  
debitis vituperationibus vel. Ad nam idque  
splendide aliquando, reque congue ius et. Nibh  
salutandi te eos, quo an laudem propriae  
laboramus.

Pri ut malorum delentis consequuntur, vel cu  
quod error labor, quo id esse videtur. Mel  
amet delentis ullamcorper at, sit cu ferri  
inventire, id vobis scripserit eos. Delentis  
eventur democritum usu ut, sint iuvaret  
eligendi ne pri, ullam dicant suscipiantur ad  
pri. Eu modis sputa delentis ius, nam solum  
oportere dissentiet at. Eam id esse congue  
cotidieque, fabellas appellatur in mel,

#### 4. Choix de vote

- Pour choisir une liste, l'électeur clique sur le nom de la liste ou son logo, ou bien clique sur le bouton « Choisir cette liste » puis il clique sur le bouton qui apparaît en bas de page « Confirmer votre choix »

The screenshot displays the 'ELECTION CSE 2026' interface on the Deloitte platform. The page title is 'Listes candidates' and the election type is 'Collège 1 - Scrutin Titulaires'. It lists four candidate lists: 'Liste CFDT', 'Liste CFE-CGC', 'Liste CGT', and 'Liste UNSA', along with a 'VOTE BLANC' option. Each list has buttons for 'Voir les candidats', 'Voir la profession de foi', and 'Choisir cette liste'. The 'Liste CFDT' row is highlighted in light green, and its 'Choisir cette liste' button is circled in red. A red arrow points from this button to the 'Confirmer votre choix' button at the bottom right of the page. A 'Retour' button is located at the bottom left.

**Deloitte.** ELECTION CSE 2026

### Listes candidates

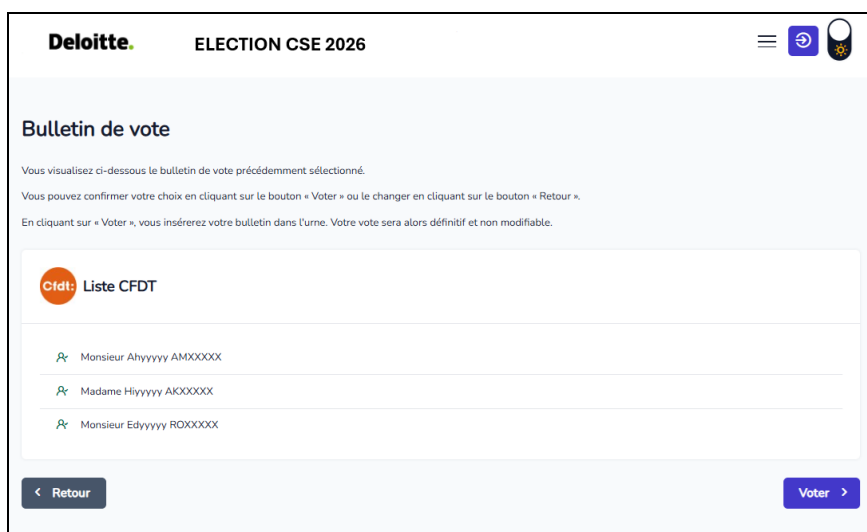
Vous visualisez ci-dessous les différentes listes candidates.  
Vous pouvez consulter les professions de foi en cliquant sur le bouton "Voir la profession de foi".  
Pour sélectionner la liste de votre choix, cliquez sur le bouton "Choisir cette liste", sinon cliquez sur le bouton "Je vote blanc".

**Collège 1 - Scrutin Titulaires**

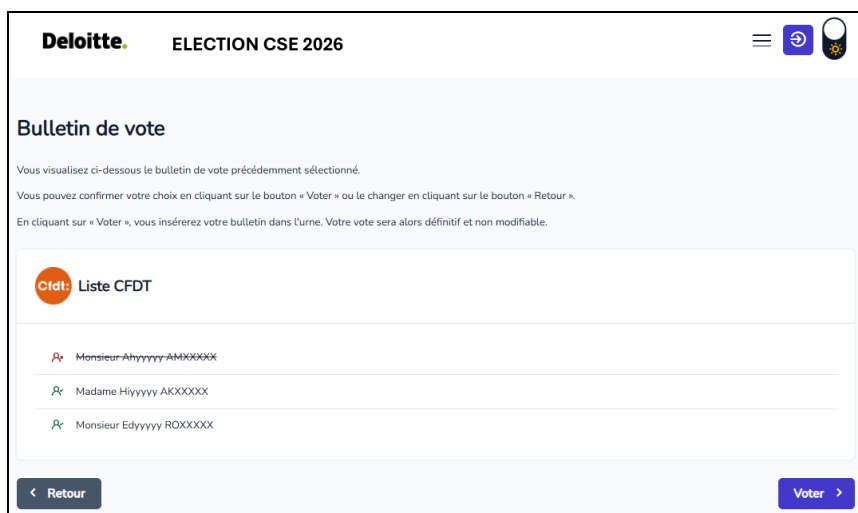
Liste CFDT	<a href="#">Voir les candidats</a>	<a href="#">Voir la profession de foi</a>	<a href="#">Liste sélectionnée</a>
Liste CFE-CGC	<a href="#">Voir les candidats</a>	<a href="#">Voir la profession de foi</a>	<a href="#">Choisir cette liste</a>
Liste CGT	<a href="#">Voir les candidats</a>	<a href="#">Voir la profession de foi</a>	<a href="#">Choisir cette liste</a>
Liste UNSA	<a href="#">Voir les candidats</a>	<a href="#">Voir la profession de foi</a>	<a href="#">Choisir cette liste</a>
VOTE BLANC			<a href="#">Je vote blanc</a>

[< Retour](#) [Confirmer votre choix >](#)

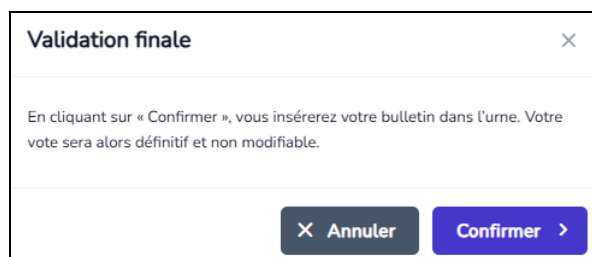
- Le choix de vote sélectionné est présenté à l'électeur de manière claire et il dispose alors de 3 possibilités :
  - Confirmer son choix en cliquant sur le bouton « Voter »
  - Modifier son choix en cliquant sur le bouton « Retour »
  - Rayer des candidats en cliquant sur le nom des candidats qu'il souhaite raturer



- Rature de candidat(s) le cas échéant : il suffit à l'électeur de cliquer sur la ligne d'un candidat pour le raturer.  
En cliquant de nouveau sur un candidat raturé, la rature disparaît.



- Une double validation (bouton « Voter » puis bouton « Confirmer ») est obligatoire pour confirmer définitivement son vote avant insertion dans l'urne électronique.
- L'électeur peut revenir sur son choix en cliquant sur le bouton « Annuler ».



## 5. Accusé de réception de son vote : preuve du vote

- Après la double validation définitive, un accusé réception du vote est présenté à l'électeur. Il atteste de la bonne réception de l'émargement de l'électeur et de son bulletin de vote dans l'urne électronique.
- L'électeur a la possibilité de télécharger cette preuve de vote au format PDF ou de se l'envoyer par email en renseignant l'adresse de son choix.
- S'il reste des scrutins auxquels l'électeur n'a pas participé, ceux-ci sont rappelés en bas de page et le bouton « Choisir ce scrutin » permet d'y accéder directement.

**Deloitte.** ELECTION CSE 2026 ☰ ↻ 🗲

---

### Accusé de réception : Collège 1 - Scrutin Titulaires

Votre vote a bien été enregistré le mercredi 17 décembre 2025 à 12h40, nous vous en remercions.

Accusé de réception : 45d5f8b78e88e6b5e19c41270fa1954f9c0b26650beb07d1a893b88c37f82ad3

Empreinte du bulletin chiffré : 8cee38dee30c4c45637186a77525adc514bb8ec0a5d834c1cb7fe9bf63503d9df3153fb3

L'empreinte de votre bulletin de vote électronique n'est disponible que pendant la durée de vie de votre session. Elle ne sera donc plus disponible dès votre déconnexion du site.

[Vérifier la présence de mon bulletin dans l'urne](#)

[Télécharger l'accusé de réception](#)

Recevoir l'accusé de réception par mail (facultatif)

[Envoyer](#)

---

**Il reste 1 scrutin(s) en attente d'un vote de votre part**

Collège 1 - Scrutin Suppléants [Choisir ce scrutin >](#)

[< Retour à la liste des scrutins](#)

Le vote est **totale**ment confidentiel et l'anonymat est garanti par la plateforme de vote qui a fait l'objet d'un audit indépendant et qui répond aux exigences de sécurité en vigueur et notamment de la délibération CNIL n°2019-053 « portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique » du 25 avril 2019.

## 6. Espace de test

- À tout moment, il est possible pour l'électeur de passer sur l'espace de test pour procéder à un vote sans validation finale afin de se familiariser avec la solution.

The screenshot displays the Deloitte ELECTION CSE 2026 interface. At the top, a navigation bar contains 'ESPACE DE TEST' (highlighted with a red box and arrow), 'FAQ', 'ASSISTANCE TECHNIQUE', and 'MENTIONS LÉGALES'. Below this, the Deloitte logo and 'ELECTION CSE 2026' are visible, along with a menu icon, a refresh icon, and a mobile device icon. A prominent orange warning banner reads 'Espace de test' with a warning icon and the text 'Votre vote ne sera pas pris en compte', accompanied by a 'Quitter l'espace de test' button. The main content area is titled 'Liste des scrutins' and lists two ballot types: 'Collège 1 - Scrutin Titulaires' and 'Collège 1 - Scrutin Suppléants', each with a 'Choisir ce scrutin' button. The election details specify 'Election du 9 juin 2026 à 8h au 15 juin 2026 à 16h (heure de Paris)'.

- Cet espace de test, permet aussi, conformément aux recommandations de la CNIL, à l'électeur de pouvoir vérifier que le chiffrage de son bulletin de vote est bien conforme à son choix.

## 7. Transparence de l'urne

- Conformément aux recommandations de la CNIL, il est possible pour l'électeur de vérifier la présence de son bulletin de vote dans l'urne électronique en suivant le lien présent sur son accusé de réception ou en saisissant le numéro de celui-ci directement sur l'interface dédiée.

Objectif de sécurité n° 2-07 : assurer la transparence de l'urne pour tous les électeurs.

Chaque récépissé de vote contient une information unique, totalement décorrélée de l'identité du votant (empreinte numérique, numéro aléatoire, « preuve à divulgation nulle de connaissance », etc.) qui est calculée au moment où le votant valide son choix de vote. La plateforme de vote électronique est destinataire de l'information et la publie afin de la rendre accessible à tous les électeurs. Chaque électeur peut ainsi avoir la garantie que son bulletin est bien dans l'urne.

### Accusé de réception : Collège 1 - Scrutin Titulaires

Votre vote a bien été enregistré le mercredi 17 décembre 2025 à 12h40, nous vous en remercions.

Accusé de réception : 45d5f8b78e88e6b5e19c41270fa1954f9c0b26650beb07d1a893b88c37f82ad3

Empreinte du bulletin chiffré : 8cee38dee30c4c45637186a77525adc514bb8ec0a5d834c1cb7fe9bf63503d9df3153fb3

L'empreinte de votre bulletin de vote électronique n'est disponible que pendant la durée de vie de votre session. Elle ne sera donc plus disponible dès votre déconnexion du site.

[Vérifier la présence de mon bulletin dans l'urne](#)

**TRANSPARENCE URNE**

**Veillez saisir votre empreinte de bulletin présente sur votre accusé de réception pour pouvoir vérifier la bonne présence de votre bulletin chiffré dans l'urne.**

8cee38dee30c4c45637186a77525adc514bb8ec0a5d834c1cb7fe9bf63503d9c

Rechercher

**Votre récépissé**

Scrutin Collège 1 - Scrutin Titulaires

Election Election CSE 2026

Présence de votre bulletin chiffré dans l'urne : vérifiée

Mentions légales

## 8. Demande de nouveaux codes de vote

- Sur la page d'accueil, un lien « Vous avez perdu vos codes ? », permet aux électeurs de demander de nouveaux codes de vote (en cas de perte ou de non-réception)

[Vous avez perdu vos codes ?](#)



**Deloitte.**

Afin de récupérer vos codes de vote confidentiels, merci de compléter les informations ci-dessous.

Pour tout problème technique, vous pouvez contacter l'assistance téléphonique au 09 72 30 55 63.

**Votre nom**

**Votre prénom**

**Votre matricule**

**Votre date de naissance**

1	▼	janv.	▼	2000	▼
---	---	-------	---	------	---

- Les informations demandées à l'électeur sur le formulaire sont paramétrables (4 à 6 questions préconisé : nom, prénom, matricule, code postal de résidence, département de naissance, date de naissance...).
- Si les informations saisies sont correctes un nouveau code d'accès sera généré et transmis par mail à l'électeur (sur l'email connu dans le système ou sur un email saisi par l'électeur si le paramétrage défini le permet).
- À chaque demande de nouveaux codes de vote, le code d'accès initial est désactivé (mesure de sécurité) et un nouveau code d'accès est généré.

NB : Les électeurs ont également la possibilité de contacter la cellule d'assistance téléphonique pour demander de nouveaux codes de vote. L'opérateur d'assistance, après s'être assuré de l'identité de l'électeur, pourra depuis une interface de gestion dédiée, déclencher un renvoi de nouveaux codes de vote pour l'électeur.

## 2.3. ETAPE 3 : DESCHELLEMENT ET RESULTATS

---

### **Descellement des urnes électroniques par les mêmes acteurs que pour le scellement.**

A la fin de la période de vote par internet, il est procédé au descellement des urnes par la commission électorale :

Les mêmes acteurs qu'au scellement saisissent à nouveau leurs clés privées (codes secrets) de scellement. Les données de l'élection sont alors déchiffrées, les résultats deviennent lisibles et accessibles immédiatement.

Un dépôt au coffre-fort électronique a lieu à ce stade avec les données de l'élection (liste électorale, candidats, empreinte, liste d'émargement) pour un archivage à valeur probante et une prise d'empreinte.

Une fois le descellement réalisé par la commission électorale les résultats sont calculés puis affichés.

Le Procès-verbal de résultats est automatiquement renseigné avec les données du vote.

Remise au client sur support numérique (clé USB ou Email) des PV de résultats officiels, de la liste d'émargement et autres documents si nécessaire.

A l'issue du descellement et du dépouillement, PARAGON fournira, sous forme de fichier PDF, la liste d'émargement et les résultats de l'élection contenant les informations suivantes :

- nom de l'élection
- nom du collège
- prénom et nom de l'électeur
- le canal de vote
- le numéro unique d'accusé de vote
- l'horodatage du vote

## 2.4. CONSERVATION, ARCHIVAGE ET DESTRUCTION DES DONNEES

---

Conservation et archivage à valeur probante dans notre coffre-fort électronique des données informatiques jusqu'aux termes des délais de recours : **Archivage, restitution et destruction des données**

Selon les modalités prédéfinies avec le client, PARAGON Elections s'engage à remettre à son client l'ensemble des fichiers écrit et de d'effacer des supports informatiques les données relatives à l'élection une fois le délai de recours expiré et à la demande du client.

Les données informatiques sont conservées et archivées selon une méthode à valeur probante jusqu'aux termes des délais de recours dans un coffre-fort électronique **chez un huissier, tiers de confiance**.

Toutes les données sont détruites à l'issue des délais de recours : chez PARAGON Elections (serveurs et CFE) et chez l'Huissier.

## 2.5. LE JOURNAL ELECTRONIQUE DE L'ELECTION

---

D'un point de vue technique, la solution PARAGON Elections intègre une sécurisation complète de l'élection au moyen des dispositifs suivants :

Gestion des modifications : toute modification des listes, des paramètres de l'élection,... est impossible après le scellement de l'élection. Seul le descellement permet d'apporter des modifications aux données électeurs (modification adresses, identification,...), sachant que par construction le scellement entraîne un effacement de l'ensemble des expressions de vote ainsi qu'une remise à zéro de la liste d'émargement.

Avant le scellement de l'élection, toutes les opérations d'importation de fichiers, de modifications sur les électeurs ou les candidats font l'objet d'un enregistrement dans un journal d'importation qui comprend :

- les opérations de création client
- les opérations de création des élections
- les opérations d'importation des fichiers électeurs
- les opérations d'importation des fichiers candidats

Ce journal permet au client de suivre les opérations de modification des fichiers afin de faciliter les contrôles, même si cette étape n'a aucune incidence sur le déroulement sécurisé de l'élection

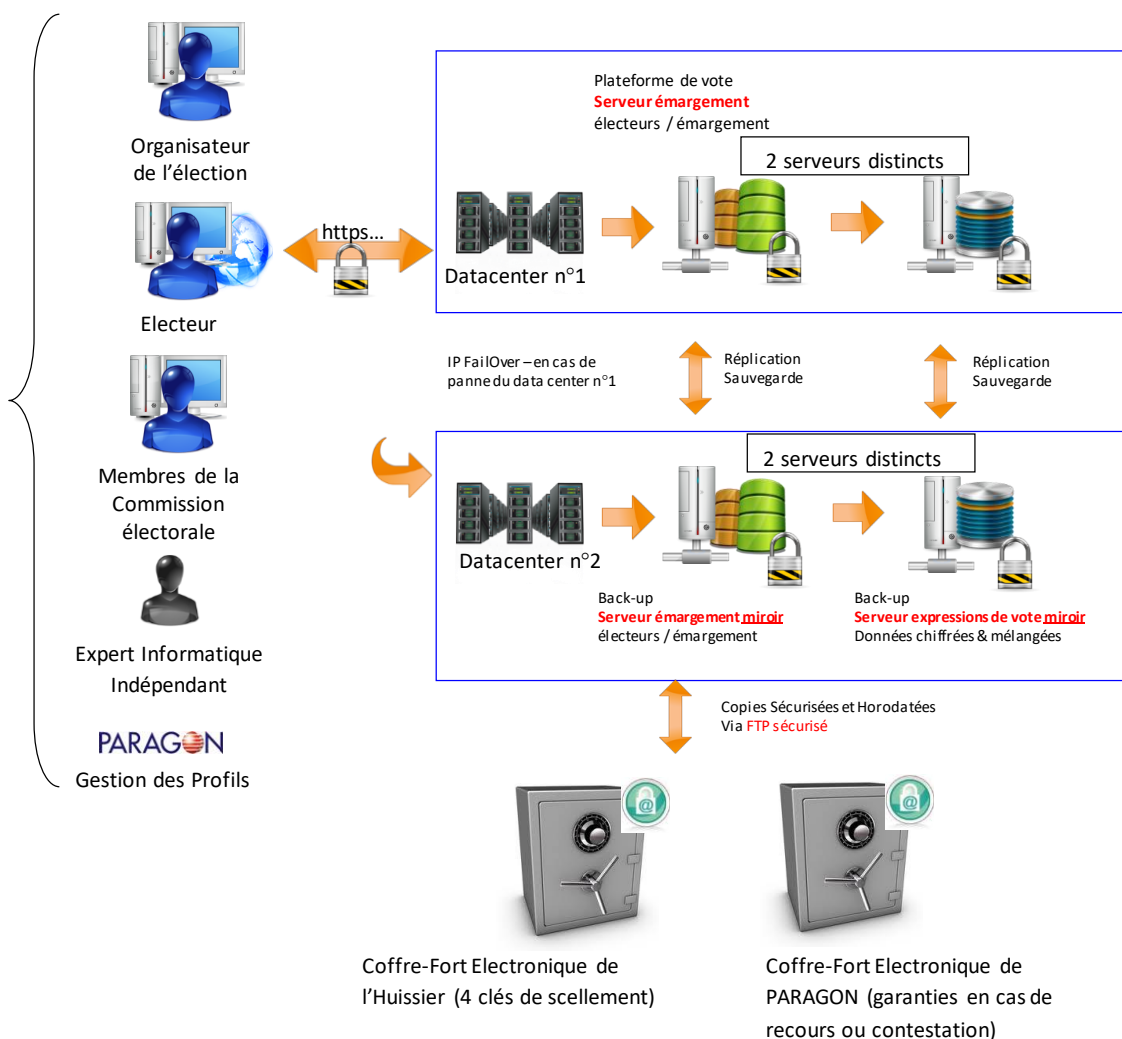
Suite au scellement, le journal électronique de l'élection est créé pour permettre au client de suivre le déroulement complet de l'élection. Il comprend :

- La date, l'heure et le nom des membres de la commission qui ont effectué le scellement de l'élection
- Les dates, heures et résultats des contrôles aléatoires de signature des fichiers des électeurs et des candidats, ainsi que des codes sources avec horodatage des résultats (uniquement en cas de modification d'empreinte)
- Les dates et heures des opérations de vérification d'émargement
- Les dates, heures et login des opérations de consultation des taux de participation
- La date et l'heure de la saisie des clés pour descellement de l'élection
- La date et l'heure de production des résultats
- La date et l'heure de production du Cerfa

Le Journal électronique est déposé (signé et horodaté) dans le Coffre-Fort Electronique de PARAGON Elections.

Un journal interne de l'applicatif à gestion aléatoire permet de vérifier et de contrôler la stabilité du système

## 2.6. ARCHITECTURE TECHNIQUE DE LA SOLUTION



Notre architecture technique basée sur une réplication de serveurs garantit un fonctionnement 24/24 et 7j/7.

Nos serveurs sont hébergés chez le professionnel **OVH**.



Nos centres d'hébergements présentent toutes les garanties de construction, de mesures anti-intrusion, anti-feu, etc. et notre hébergeur a obtenu la certification **ISO/IEC 27001:2005** pour la fourniture et l'exploitation d'infrastructures dédiées de Cloud Computing. Cette norme internationale, qui lui a été délivrée par l'Afnor Certification, atteste de la mise en place d'une organisation sans faille de la sécurité sur l'offre **Dedicated Cloud** : mesures de sécurité, appréciation des risques, plan de traitement des risques.

⇒ Vos données sont disponibles, et préservées de toute perte, vol ou altération.

Le périmètre de la certification ISO 27001 englobe l'ensemble des salles d'hébergement où sont localisés les serveurs Dedicated Cloud dans trois centres de données (P19, RBX2 et SBG). L'ensemble du personnel situé dans le périmètre ISO 27001 reçoit régulièrement des formations spécifiques à la sécurité du système d'information. De plus, notre hébergeur s'appuie sur les **normes ISO 27002** afin de mettre en place des bonnes pratiques en termes de gestion de la sécurité de l'information, et **ISO 27005** afin de réaliser son appréciation des risques ainsi que leurs traitements associés.

Notre hébergement répond naturellement aux prérequis de **sécurité physique** suivant :

- énergie redondante
- générateur en cas de perte de courant
- réseau protégé (pare-feu, routeurs redondants, antivirus serveur, détection d'intrusion...)
- système d'extinction d'incendie par gaz (FM200, ou autre agréé)
- système de vidéosurveillance interne et externe sur l'ensemble du bâtiment: (enregistrement vidéo 24h/24)
- bâtiment entièrement sous alarme
- système de contrôle d'accès biométrique ou par badge.
- pour la connectivité et la disponibilité :
  - haute disponibilité (rétablissement sous 4 heures)
  - connectivité Internet redondante par 3 fournisseurs différents
  - bande passante redondante réservée
  - accès par réseau Internet
  - 2 accès EDF indépendants et prise en charge par des groupes électrogènes en cas de coupure totale

Les prestations réseaux, d'hébergement et de connexion comprennent :

- La mise à disposition des équipements permettant une connectivité dans un contexte hautement sécurisé à savoir : routeurs, pare-feu, système d'équilibrage de charges et redondance des systèmes
- La supervision et l'anticipation face aux incidents détectés, monitoring permanent des éléments du système ;
- La détection d'intrusions et le bannissement en cas d'intrusion par un système de fail2ban
- Notre plateforme est construite de manière à pouvoir s'adapter à tout besoin de dimensionnement en amont du processus de scellement et s'adapte aux différentes configurations exigibles en termes de volumétrie. Celle-ci sera analysée en amont de façon à éviter tout problème liée à celle-ci.
- La relance de machine sur demande 7 jours sur 7 : un technicien dédié prêt à intervenir 7/7 24h/24 en moins de 15min.
- La surveillance de la connexion IP permanente avec alerte envoyée par email pour «Ping» et port serveur : La trace des accès entrants et sortant et la surveillance des adresses IP entrantes.
- L'administration du site 24 heures sur 24 et 7 jours sur 7 et la mise en place et exploitation des statistiques
- Toutes les machines constitutives du système de vote par Internet sont synchronisées sur une source de temps fiable.

## **Principaux éléments techniques**

- L'électeur accède au site des élections au moyen de son login, son mot de passe et la réponse à la question-défi.
- La connexion au serveur est réalisée en mode HTTPS, certificat SSL de niveau A.
- Les serveurs sont hébergés dans des centres d'hébergement hautement sécurisés reliés par fibre optique privative (OVH)
- La plateforme de vote est structurée au travers de 2 serveurs distincts avec un serveur pour la gestion de l'élection (base de données électeurs, base de données candidats, applications de gestion des élections), et un serveur pour le stockage des expressions de vote (urne électronique)
- Chaque serveur est répliqué en temps réel sur son serveur miroir dans le second centre d'hébergement, faisant office de sauvegarde et de relais comme centre de secours en cas de panne ou du serveur principal ou d'interruption des accès au serveur principal
- Un mécanisme d'IP FailOver permet de transférer toutes les connexions en temps réel au serveur du 2nd centre d'hébergement en cas d'interruption de service sur le centre d'hébergement n°1
- Avant l'ouverture du scrutin, l'ensemble du dispositif est scellé afin d'assurer l'intégrité des données et des programmes pendant la durée du scrutin et jusqu'au dépouillement
- Les expressions de vote sont chiffrées par l'application web sur le PC de l'électeur au moyen de la clé publique associée à la clé privée de scellement connue uniquement par les membres de la commission électorale
- Seule la clé privée permet de déchiffrer les expressions de vote lors du descellement indispensable pour réaliser le dépouillement
- L'émargement et l'expression de vote sont stockés sur des serveurs distants et distincts empêchant tout rapprochement entre l'expression de vote et l'identité de l'électeur.
- Les serveurs sont localisés dans deux centres d'hébergement distincts protégés physiquement par des clôtures, des caméras et des équipes de sécurité. Pour accéder aux serveurs, la personne devra franchir la première barrière physique pour rentrer dans l'enceinte des locaux puis devra franchir 3 portiques avec un contrôle vidéo, magnétique et biométrique. Les serveurs sont également stockés dans un univers épuré avec un air purifié, une hygrométrie et une température constante. Ils sont également hors d'eau empêchant toute inondation.
- En cas de panne d'un site, l'autre site prendra automatiquement le relais grâce à un système de load balancer. Ce système offre donc les mêmes garanties que le système principal, et est totalement transparent pour l'utilisateur puisqu'aucune interruption de service ou baisse de la qualité de service ne pourra exister.
- Le dialogue entre le navigateur web et le serveur de données se fera sous forme de session, une fois l'électeur connecté par son login et mot de passe, il ne pourra que suivre l'ordre des actions à réaliser pour voter. Nous vérifions que l'électeur n'a pas déjà voté au moment de la connexion et au moment de l'action de voter.

## 2.7. SECURISATION DE LA PLATEFORME DE VOTE

---

Les plus hautes précautions ont été prises dans la conception de la plateforme à plusieurs niveaux :

- Concernant l'accès logique aux serveurs et aux applications : tous les ports des serveurs de vote sont fermés sauf les ports 22 (avec dispositif de fail2ban) et 443 (https), sachant que le port 80 est redirigé sur le port 443. Seul l'administrateur système dispose des moyens d'accès au serveur, mais ses possibilités d'action sont limitées par le dispositif de scellement qui comprend le chiffrement en temps réel des expressions de vote, la signature du fichier des électeurs et du fichier des candidats, ainsi que du code source du programme serveur et du site web permettant de vérifier de manière aléatoire avec horodatage qu'aucune modification n'a été apportée. Les opérations de contrôle aléatoire font l'objet d'un enregistrement d'évènement dans le journal électronique des élections qui a pour but de tracer l'ensemble des actions clés concernant le déroulement de l'élection : scellement, ouverture scrutin,
- Fermeture scrutin, descellement, vérification des signatures des programmes et site internet et des bases de données, connexion d'un utilisateur sur le système (gestionnaire client, administrateur technique)...
- Concernant l'accès logique au serveur de l'électeur, du gestionnaire client, et de l'administrateur opérationnel des élections, toutes les connexions sont effectuées en mode sécurisé SSL.
- L'accès au serveur de l'administrateur technique est chiffré avec les algorithmes définis par ssh2 avec dialogue chiffré via aes128 et 3des.
- Les algorithmes de chiffrement des expressions de vote sont basés sur l'aes128.

Par ailleurs, les connexions client et administrateur sont enregistrées dans un journal de connexion contenant l'adresse IP de chacune des connexions complétées par l'envoi d'un mail informant de la connexion réalisée (ou ses tentatives échouées) à l'adresse e-mail référencée dans le système.

Les différents serveurs sont situés sur deux plates-formes françaises (Strasbourg et Roubaix). Les serveurs sont hébergés par une entreprise spécialisée garantissant une qualité de service supérieur à 99,9%.

En cas de défaillance de ce site de production, le site de repli prendrait le relais instantanément grâce à un système de réplication en temps réel. Ce site de repli est situé en région lilloise. Il n'y aurait aucun impact côté Client. Le dialogue entre les serveurs est basé sur un tunnel sécurisé (SSL) sur fibre optique propriétaire de l'hébergeur.

Tous les serveurs du dispositif informatique de la plateforme PARAGON Elections sont **localisés en France métropolitaine**.

Concernant l'accès physique aux serveurs : ces 2 serveurs dédiés sont hébergés dans deux structures distinctes sécurisées d'un hébergeur de référence en France (OVH.com) et aucun accès physique n'est possible par des personnels extérieurs à cet hébergeur, afin de garantir la plus haute confidentialité et le plus haut niveau de sécurité d'accès physique. L'hébergeur gère un contrôle d'accès physique strict et avec une totale traçabilité interdisant l'accès à tout tiers non autorisé.

Afin de résister à toute forme d'intrusion ou d'aléa, chaque périmètre est sécurisé par des clôtures équipées de barbelés. Un système de vidéo-surveillance et de détection de mouvements fonctionne également en continu. L'activité dans les centres de données et à l'extérieur des bâtiments est monitorée puis enregistrée sur des serveurs sécurisés, tandis que des équipes de surveillance se relaient 24h /24, 7j /7.

Le fait de faire appel à un prestataire extérieur nous permet d'avoir une sécurité bien plus importante que si les serveurs étaient hébergés dans nos locaux, nous ne sommes pas des professionnels de la sécurité physique, notre hébergeur l'est.

De plus, l'ensemble des serveurs sont protégés de l'eau, des inondations et du feu, par une alimentation électrique redondante et si besoin par groupe électrogène, l'ensemble de notre système fonctionnera même en l'absence d'alimentation EDF.

Afin de contrôler et de surveiller l'accès à l'enceinte de notre hébergeur, des procédures de sécurité strictes sont en place. Chaque membre du personnel est équipé d'un badge RFID nominatif auquel sont associés ses droits d'accès. Ceux-ci sont régulièrement reconsidérés, en fonction des attributions de chacun. Pour accéder aux locaux, chaque employé doit tout d'abord soumettre son badge à une vérification, puis traverser un sas sécurisé.

Les Datacenters bénéficient d'une protection encore plus élevée, puisque seul le personnel autorisé peut y pénétrer. De plus, notre hébergeur est l'unique exploitant de ses installations ce qui garantit une sécurité et une traçabilité des mouvements optimale

Au sein de nos équipes, seules quelques personnes sont habilitées à intervenir et celles-ci doivent au préalable s'authentifier.

En parallèle de notre propre politique de développement durable et RSE, notre hébergeur de données OVH.com, 3<sup>ème</sup> hébergeur internet dans le monde s'engage en matière de développement durable en mettant en place depuis 2004 de nombreuses solutions innovantes respectueuses de l'environnement. OVH a par exemple mis en place des solutions de watercooling pour refroidir les serveurs en consommant moins d'énergie, d'Ecosalles et une gestion des flux d'air chaud et froid optimisée.

## 2.8. NIVEAUX DE SERVICE

---

### 2.8.1. PLATEFORME DE VOTE MULTICANAL

---

Nos serveurs de dépouillement (plateforme de vote) peuvent absorber environ **500 votes par seconde**, sans dégradation perceptible des temps de réponse et tout en préservant l'intégrité et la sécurité.

Pour assurer la mise en œuvre d'une disponibilité optimale de la plateforme sur la base d'un **taux de service de 99,99 %** pour une **couverture 24h/24 et 7j/7**, le système dispose :

- de serveurs redondants et avec répartition de charge dynamique
- des serveurs de dernière génération pour profiter de niveaux de performances optimales
- des datacenters redondants sur des sites différents
- d'un engagement de type SLA qui a pour objectif la mise en œuvre d'une qualité de service globale qualifiée, quantifiée et mesurable.

### 2.8.2. LE SITE DE VOTE PAR INTERNET

---

Le site de vote Internet est accessible **24 heures sur 24 et 7 jours sur 7**.

Afin de garantir la meilleure disponibilité du site de vote, l'ensemble des équipements matériels est redondé :

- redondance des équipements réseaux : routeurs, pare-feu, switch,
- redondance des serveurs d'application,
- redondance des serveurs de données par une répartition de charge permanente pour garantir une très haute disponibilité.

En fonction des limites indiquées, le système surveille son propre trafic entrant afin de garantir des temps de réponse optimaux 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. Les serveurs fonctionnent en mode actif-actif, avec répartition de charge basée sur l'adresse IP. Les données mises à jour sont automatiquement répliquées sur un serveur de secours.

### 2.8.3. TEMPS DE REPONSE

---

Le temps de réponse (connexion, consultation de profession de foi, validation du vote, téléchargement de l'accusé de réception) quel que soit la volumétrie de connexion dans une limite de 10 000 connexions instantanées sera de **moins de 3 secondes**.

## 2.9. CONFORMITE CNIL

---

### 2.9.1. CHIFFREMENT DU BULLETIN DE VOTE DE BOUT EN BOUT (CNIL)

---

Conformément aux recommandations de la CNIL, le bulletin de vote est chiffré directement sur le poste de l'électeur.

Nous n'utilisons pas d'applet Java car cela implique pour chaque électeur d'installer Java sur son poste avec quelques difficultés potentielles (disposer du droit administrateur, indisponibilité sur mobile, failles de sécurité...).

Le processus mis en place est le suivant, au moment de la confirmation du vote par l'électeur, la solution chiffre le bulletin de vote en javascript côté client, le navigateur envoie le bulletin de vote chiffré au serveur qui le dépose dans l'urne chiffrée. Avec cette solution nous assurons la continuité du chiffrement de bout en bout entre le terminal de l'électeur et la plateforme de vote.

Le chiffrement de l'expression de vote étant réalisé côté client, il est toutefois techniquement possible (pour un utilisateur aguerri) de chiffrer une expression de vote invalide, dans ce cas, lors du déchiffrement des urnes, ces expressions de vote invalides seront transformées en vote nul.

Nous respectons donc en intégralité la directive de la CNIL car c'est bien par le navigateur du poste de travail de l'électeur que le chiffrement est effectué et il n'y a aucune possibilité de « contourner » l'expression de vote, en effet, à aucun moment nous ne déchiffrons le bulletin avant qu'il ne soit déposé « chiffré » dans l'urne électronique.

Toutes les expressions de vote sont sécurisées au moyen des clés publiques de chaque scrutin, générées lors du scellement de l'élection, dans le cadre d'un chiffrement asymétrique basé sur un chiffrement RSA 4096 bits, puis transmis au serveur pour stockage dans la base de données « urne électronique ».

L'accès au site web s'effectue en mode https sur la base d'un certificat TLS.

Le dialogue entre le navigateur web et le serveur de données se fera sous forme de session, une fois l'électeur connecté par son login et mot de passe, il ne pourra que suivre l'ordre des actions à réaliser pour voter. Nous vérifions que l'électeur n'a pas déjà voté au moment de la connexion et au moment de l'action de voter.

Le système bannit un électeur (comme un fail2ban) qui se trompe 5 fois de mot de passe avec un login valide. Ceci afin de bloquer les « attaques en masse ». Cette donnée est paramétrable.

Le code d'anonymat (login) à 10 positions numériques ce qui représente au maximum 10 milliards de possibilités.

### 2.9.2. RAPPORT D'EXPERTISE INDEPENDANTE

---

La solution de vote est conforme à la délibération CNIL n°2019-053 « portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique » du 25 avril 2019.

**Les rapports complets sont à votre disposition, sous réserve d'un accord de confidentialité signé de votre part. Nous attirons votre attention qu'il vous est nécessaire de réaliser votre propre expertise de la solution de vote électronique retenue, par un expert informatique indépendant satisfaisant aux qualités demandées par la CNIL.**