

envoyé : 3 octobre 2026 à 05:56

de : mitchell.john@orange.fr

à : contact@choisir2027.fr

cc : parti-socialiste@parti-socialiste.fr, rgpd@choisir2027.fr

Objet : LETTRE OUVERTE - Primaire Choisir 2027 — garanties techniques, anonymat et vérifiabilité du vote électronique

Vouvray-sur-Loir le 03/10/2026

Bonjour,

Je souhaite participer à la primaire Choisir 2027. En tant qu'informaticien ayant travaillé depuis les années 1980 sur des systèmes informatiques, notamment des expériences de vote sur Minitel, je m'interroge depuis longtemps sur une difficulté fondamentale du vote électronique : comment garantir simultanément **l'anonymat du vote, son intégrité et sa vérifiabilité** ?

Ma démarche ne consiste nullement à mettre en doute l'honnêteté des organisateurs ou des personnes chargées du scrutin. Au contraire, je considère qu'un bon système électoral doit pouvoir démontrer sa fiabilité indépendamment de la confiance accordée aux personnes qui l'organisent.

Le site Choisir 2027 indique que le vote est « strictement personnel et secret ». Je souhaiterais donc connaître précisément les garanties techniques et organisationnelles permettant également de vérifier que chaque suffrage exprimé est correctement enregistré et que le résultat proclamé correspond exactement aux suffrages exprimés.



### **Pourriez-vous, s'il vous plaît, répondre aux questions suivantes ?**

#### **1. Quel système et quel prestataire ?**

Quel prestataire développe, héberge et exploite la plateforme de vote électronique de Choisir 2027 ? Quelle solution logicielle est utilisée et où sont hébergés les serveurs pendant le scrutin ?

#### **2. Le code source est-il auditable ?**

Le code source du logiciel de vote a-t-il fait l'objet d'un audit indépendant ? Si oui, par quel organisme ou quels experts, à quelle date et selon quel référentiel ? Le rapport d'audit complet ou une synthèse technique est-il accessible au public et aux représentants des candidats ?

#### **3. Comment vérifier que le programme audité est réellement celui qui fonctionne le jour du vote ?**

Quels mécanismes permettent de garantir que le code exécuté sur les serveurs pendant toute la durée du scrutin est strictement identique à la version ayant fait l'objet de l'audit ? Utilisez-vous notamment des empreintes cryptographiques, signatures numériques, scellements ou procédures équivalentes permettant de détecter toute modification ?

#### **4. Comment l'identité de l'électeur est-elle séparée de son bulletin ?**

Le système doit vérifier qu'une personne possède le droit de voter et qu'elle ne vote qu'une seule fois, tout en rendant impossible l'association ultérieure de son identité avec son choix. Quel mécanisme technique

assure cette séparation ? Existe-t-il une preuve vérifiable que la liste d'émargement ne peut pas être rapprochée du contenu de l'urne électronique ?

**5. L'électeur peut-il vérifier que son vote a réellement été pris en compte ?**

Après avoir voté, l'électeur reçoit-il un identifiant, récépissé ou élément cryptographique anonyme lui permettant de vérifier que son bulletin est bien présent dans l'urne et sera inclus dans le dépouillement, sans que cet élément permette de découvrir ou de prouver à un tiers pour qui il a voté ?

**6. Comment garantir l'intégrité du bulletin de bout en bout ?**

Quels mécanismes permettent de démontrer que le choix effectué sur le terminal de l'électeur est exactement celui qui est enregistré, conservé puis comptabilisé, sans modification possible entre ces différentes étapes ? Le système offre-t-il une forme de vérifiabilité de bout en bout (*end-to-end verifiability*) ?

**7. Comment les candidats et leurs représentants peuvent-ils contrôler le scrutin ?**

Les candidats peuvent-ils désigner des experts ou assesseurs disposant d'un accès aux éléments techniques nécessaires au contrôle du scrutin ? Peuvent-ils assister au scellement initial, surveiller les opérations, contrôler le dépouillement et vérifier indépendamment les résultats ?

**8. Quelles traces vérifiables sont conservées ?**

Quels journaux techniques, empreintes cryptographiques, preuves de scellement et autres éléments d'audit sont conservés ? Comment garantit-on leur intégrité et leur horodatage sans conserver d'information permettant de lever le secret du vote ? Combien de temps ces éléments sont-ils conservés ?

**9. Quelle procédure existe en cas de contestation ?**

Si un candidat, un électeur ou un expert relève une anomalie, quelle instance indépendante peut être saisie ? Quels sont les délais et modalités d'une réclamation ? Une expertise informatique contradictoire peut-elle être demandée et, si nécessaire, ordonnée ?

**10. Peut-on procéder à l'équivalent d'un recomptage ?**

Avec des bulletins papier, en cas de contestation, il est possible de rouvrir les urnes et de recompter les suffrages devant plusieurs personnes. Quel est l'équivalent prévu pour Choisir 2027 ? Peut-on refaire indépendamment le dépouillement à partir de données électorales cryptographiquement scellées et vérifier que le résultat obtenu est identique, tout en préservant définitivement le secret des votes ?

Ces questions ne sont pas théoriques pour moi. Après plus de quarante années d'informatique, je reste convaincu qu'en matière électorale la confiance ne devrait jamais remplacer la possibilité de contrôle.

Si votre système apporte des réponses solides à ces dix questions, je serais au contraire très heureux de les connaître et de pouvoir expliquer autour de moi pourquoi le scrutin est techniquement vérifiable.

Je vous remercie donc par avance de bien vouloir me communiquer les réponses ainsi que, si possible, les documents techniques, rapports d'audit, règlement du scrutin ou références permettant de les vérifier.

Bien cordialement,

**Citizen John MITCHELL** avec l'aide de ChatGPT

<https://cxir.fr>