

Université Cheikh Anta DIOP



Ecole Supérieure Polytechnique Département Génie Informatique

***SunuElection** : Document sur les exigences*

Membre : Ouleymatou Sadiya CISSÉ

Professeur : Dr Doudou FALL

Année académique 2024-2025



1. Objectif du système

SunuElection est un système de vote électronique sécurisé destiné à remplacer les méthodes de vote papier dans les contextes académiques et institutionnels. Son objectif est d'assurer un processus électoral **fiable, confidentiel, anonyme, et traçable**, tout en respectant les principes de transparence et de démocratie.

Le système permet aux électeurs de s'authentifier via un compte personnel, puis de voter en ligne à l'aide d'un bulletin chiffré. Le chiffrement se fait à l'aide d'un algorithme asymétrique (**RSA**), assurant que personne, pas même l'administrateur, ne peut relier un électeur à son vote.

Les scrutateurs disposent d'un module d'audit sécurisé permettant la vérification de l'intégrité du processus, via des journaux signés et horodatés. L'administration, quant à elle, accède uniquement à des résultats agrégés sans information nominative.

SunuElection garantit également la résistance aux fraudes et intrusions en intégrant le chiffrement des données, l'usage du protocole **HTTPS**, le hachage des mots de passe (**Bcrypt**) et un contrôle strict des accès par rôles (**DAC**).

2. Exigences fonctionnelles

Voici les exigences fonctionnelles selon la méthode **MoSCoW** et les principes **INVEST** :

Type d'utilisateur	Actif	Importance	User Story
Électeur	Identifiants	Must	En tant qu'électeur, je veux pouvoir m'authentifier pour accéder à l'espace de vote.
Électeur	Bulletin de vote	Must	En tant qu'électeur, je veux pouvoir voter de façon confidentielle via l'interface web.
Électeur	Base des votes	Must	En tant qu'électeur, je veux être sûr que mon vote est enregistré et pris en compte.
Admin	Liste électorale	Must	En tant qu'administrateur, je veux pouvoir charger la liste des électeurs avant le scrutin.



Admin	Résultats	Must	En tant qu'administrateur, je veux pouvoir voir les résultats finaux sans lien avec les identités.
Scrutateur	Logs d'audit	Should	En tant que scrutateur, je veux pouvoir consulter les journaux pour vérifier l'intégrité du vote.
Électeur	Notification	Could	En tant qu'électeur, je veux recevoir une confirmation que mon vote a bien été pris en compte.

3. Analyse des menaces

Attaquants possibles :

- **Hackers externes** : tentent d'accéder au serveur pour modifier les votes.
- **Utilisateurs malveillants** : électeurs qui essaient de voter plusieurs fois.
- **Administrateur corrompu** : pourrait tenter d'accéder à des données sensibles ou de manipuler les résultats.
- **Man-in-the-Middle** : interception des données en transit.

Non-menaces (hypothèses) :

- Le serveur est hébergé dans une salle sécurisée et contrôlée.
- Les administrateurs sont formés et dignes de confiance dans des conditions normales.

4. Objectifs de sécurité

Actif	Partie prenante	Préjudice possible	Objectif de sécurité	Catégorie
Bulletin de vote	Électeur	Atteinte à l'anonymat	Le système doit empêcher tout lien entre électeur et bulletin	Confidentialité
Résultat agrégé	Admin	Manipulation du score final	Le système doit garantir l'intégrité du décompte final	Intégrité
Identifiants	Électeur	Usurpation d'identité	Le système doit sécuriser les	Confidentialité



			identifiants et empêcher leur fuite	
Journaux d'audit	Scrutateur	Altération ou suppression des preuves	Le système doit signer et horodater les logs pour garantir leur fiabilité	Intégrité
Clé privée de dépouillement	Système	Exfiltration par un attaquant	Le système doit restreindre l'accès à la clé privée et la stocker de façon sécurisée	Confidentialité