Université Cheikh Anta DIOP

Ecole Supérieure Polytechnique

Département Génie Informatique

Rapport Final

Membre : Ouleymatou Sadiya CISSÉ

Professeur : Dr Doudou FALL

Année académique 2024-2025

Introduction

Ce rapport final présente l'état d'avancement du projet *SunuElection*, en mettant l'accent sur la mise en œuvre des exigences fonctionnelles, la sécurité du système, ainsi que les mécanismes d'assurance qualité. Il fournit un aperçu des fonctionnalités livrées, des tests réalisés, et des mesures techniques adoptées pour garantir l'intégrité, la confidentialité et la traçabilité du processus de vote électronique.

1. Tableau MoSCoW / INVEST

Type d'utilisateur	Fonction	Importance	User Story	Implémenté)
Électeur	Authentification	Must	En tant qu'électeur, je veux pouvoir m'authentifier pour accéder à l'espace de vote.	Oui
Électeur	Bulletin de vote	Must	… je veux pouvoir voter de façon confidentielle via l'interface web.	Oui
Électeur	Base des votes	Must	… je veux être sûr que mon vote est enregistré et pris en compte.	Oui
Admin	Import liste électorale CSV	Must	… je veux pouvoir charger la liste des électeurs avant le scrutin.	En attente
Admin	Résultats agrégés	Must	… je veux pouvoir voir les résultats finaux sans lien avec les identités.	Oui

Scrutateur	Consultation des journaux	Should	… je veux pouvoir consulter les journaux pour vérifier l'intégrité du vote.	Oui
Électeur	Notification de vote	Could	… je veux recevoir une confirmation que mon vote a	Oui
			bien été pris en compte.	

2. Satisfaction des Exigences de Sécurité

- **Autorisation**
  Le modèle d'autorisation adopté est basé sur le **Discretionary Access Control (DAC)**, implémenté sous la forme d'un **contrôle d'accès basé sur les rôles (RBAC)**. Trois rôles principaux sont définis et enregistrés en base de données : **ADMIN**, **USER** et **SCRUTATEUR**. L'application des règles de sécurité s'appuie sur des **annotations telles que @PreAuthorize et @Secured**, ainsi que sur un **filtre JWT** pour restreindre l'accès aux ressources sensibles. Les **modifications de rôles peuvent être effectuées dynamiquement via l'interface d'administration**, avec une prise d'effet immédiate.

- **Authentification**
  L'authentification des utilisateurs repose sur un **identifiant (login) et un mot de passe haché** à l'aide de l'algorithme **Bcrypt avec un coût de 10 rounds**, garantissant ainsi la robustesse du stockage des identifiants. Le système utilise des **JSON Web Tokens (JWT)** signés en **HS512**, avec une **durée de validité de 15 minutes** pour les jetons d'accès, et un **jeton de rafraîchissement valable 7 jours**, assurant un bon équilibre entre sécurité.

- **Audit/Responsabilité**
  Le système d'audit repose sur une **table dédiée nommée audit_log**, contenant les champs suivants : *utilisateur, action, détails, horodatage, hash cumulatif* et *signature RSA-PSS*. Afin de garantir l'intégrité des journaux, un **chaînage cryptographique par SHA-256** est mis en place, complété par une **signature numérique** permettant de détecter toute tentative de modification. Un **endpoint sécurisé /api/audit/verify** permet de lancer à tout moment une vérification complète de l'intégrité des journaux.

- **Confidentialité**
  La confidentialité des votes est assurée par un **chiffrement côté client à l'aide d'une clé publique RSA de 2048 bits**, garantissant ainsi la protection des données avant leur transmission. Toutes les communications entre le client et le serveur s'effectuent via le **protocole sécurisé HTTPS**. Par ailleurs, aucune **information personnelle identifiable**

(PII) n'est enregistrée dans les logs associés aux bulletins de vote, ce qui renforce la protection de la vie privée des électeurs.

- **Intégrité**
  L'intégrité des données est assurée à plusieurs niveaux. D'une part, des **contraintes JPA** et des **clés étrangères** sont utilisées pour garantir la cohérence des relations en base de données. D'autre part, les journaux d'audit sont protégés par un **hash cumulatif couplé à une signature numérique**, permettant de détecter toute modification non autorisée. Enfin, une **vérification systématique des signatures de vote** est mise en place afin d'assurer l'authenticité et la non-altération des bulletins enregistrés.
- **Gestion des secrets**

Secret	Création / Rotation	Stockage	Effacement
Mot de passe utilisateur	Choisi / réinit.admin	Bcrypt en BD	Réécriture + logs filtrés
Clé secrète JWT	Variable d'env.	application.properties externalisé	Suppression + redémarrage
Paire RSA serveur	Générée au déploiement	Keystore.p12 protégé	Rotation annuelle, ancien fichier supprimé

- **Assurance et Tests**

Niveau	Outils	Métriques
Unitaire	JUnit 5, Mockito	29 tests – couverture lignes : 78 %
Intégration	SpringBootTest + H2	12 tests
Sécurité	Spring Security Test, OWASP ZAP (passive)	0 alerte haute
Statique	SpotBugs 4.7.3 + FindSecBugs 1.12	82 Bugs, 0 erreur

- **Statut des Tâches**

ID	Tâche	Volet	Statut
A-01	Journal d'audit + UI	Audit	Réalisé
A-02	Intégrité log (hash + sig)	Audit	Réalisé
A-03	RSA clé publique API	Audit	Réalisé
A-04	Vote chiffré client	Audit	Réalisé
A-05	Auth JWT & refresh	Authentification	Réalisé

A-06	Routes protégées rôles	Autorisation	Réalisé
A-07	Page scrutateur / admin résultats	Audit/Autorisation	Réalisé
A-08	Import CSV électeurs	Autorisation	Non Réalisé
A-09	Notification de vote email	UX	Réalisé

Deux ressources complémentaires sont mises à disposition pour la vérification de la qualité et de la documentation du projet :

- Le **rapport d'analyse statique généré par SpotBugs**, accessible à l'emplacement target/spotbugs.html.
- La **documentation de l'API REST**, disponible via l'interface Swagger à l'adresse suivante : http://localhost:8080/api/swagger-ui.html.

Code source

Le code source de l'application est disponible sur le dépôt GitHub suivant :

https://github.com/Ouleymatou14/SunuElection.git

Conclusion

Le projet *SunuElection* a atteint ses objectifs principaux, avec la réalisation des fonctionnalités critiques et l'intégration de mécanismes de sécurité solides. Malgré quelques tâches encore en attente, le système présente un haut niveau de fiabilité, soutenu par des tests rigoureux et une documentation technique complète. Il constitue ainsi une base robuste pour un déploiement sécurisé d'une solution de vote en ligne.