Une version mise à jour de votre document sur les exigences, indiquant clairement les exigences qui ont été mises en œuvre et celles qui sont encore en attente ;

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type d'utilisateur** | **Actif** | **Importance** | **User Story** | **Terminé** |
| Électeur | Identifiants | Must | En tant qu’électeur, je veux pouvoir m’authentifier pour accéder à l’espace de vote. | Oui |
| Électeur | Bulletin de vote | Must | En tant qu’électeur, je veux pouvoir voter de façon confidentielle via l’interface web. | Oui |
| Électeur | Base des votes | Must | En tant qu’électeur, je veux être sûr que mon vote est enregistré et pris en compte. | Oui |
| Admin | Liste électorale | Must | En tant qu’administrateur, je veux pouvoir charger la liste des électeurs avant le scrutin. | En Attente |
| Admin | Résultats | Must | En tant qu’administrateur, je veux pouvoir voir les résultats finaux sans lien avec les identités. | Oui |
| Scrutateur | Logs d’audit | Should | En tant que scrutateur, je veux pouvoir consulter les journaux pour vérifier l’intégrité du vote. | Oui |
| Électeur | Notification | Could | En tant qu’électeur, je veux recevoir une confirmation que mon vote a bien été pris en compte. | En Attente |

Document d’Assurance – SunuElection

*(Sprints – volets Audit & Authentification/Autorisation)*

Ce document résume la stratégie qualité appliquée, les outils utilisés et l’état exact des travaux réalisés à la date d’aujourd’hui.

1. Couverture des Volets Fonctionnels

| Volet | Stories livrées | État |
| --- | --- | --- |
| Audit | - Journal complet (CRUD, filtrage) - Hachage SHA-256 signé pour détection d’altération - UI admin + scrutateur - | ✅ Done |
| Authentification | - Login/Registration JWT - Hash Bcrypt (10 rounds) - Refresh token | ✅ Done |
| Autorisation | - Rôles ADMIN / USER / SCRUTATEUR -  @PreAuthorize   sur routes sensibles - Redirections front en fonction des rôles | ✅ Done |

2. Pyramide de Tests

| Niveau | Outils | Cas & Métriques |
| --- | --- | --- |
| Unitaire | JUnit 5, Mockito | 29 tests |
| Intégration | @SpringBootTest   + H2 | 12 tests (flux REST ↔ Service ↔ Repo) |
| Sécurité | Tests négatifs + OWASP ZAP (passive) | SQLi, XSS, CSRF : 0 alerte haute |

2.1 Exemples de Cas Clés

* CryptoServiceTest
  + Vérifie signature & vérification RSA, chiffrement / déchiffrement.
* VoteEndpointAuthZIT
  + USER appelle

/api/admin/candidates

 ⇒ 403.

* AuditIntegrityIT
  + Modifie un log manuellement ⇒ hash global divergent, la vérification échoue.
* JwtExpiryIT
  + Avance horloge 1 h ⇒ token expiré ⇒ 401.

3. Mesures Spécifiques Audit

| Exigence | Implémentation | Vérification |
| --- | --- | --- |
| Traçabilité | Entrées BD  audit\_log   (user, action, date) | IT + UI |
| Intégrité | SHA-256 cumulatif + signature RSA | Test unité  AuditIntegrityTest |
| Confidentialité | Aucun PII dans log de vote | Revue code |

4. Mesures Spécifiques AuthN / AuthZ

| Exigence | Implémentation | Vérification |
| --- | --- | --- |
| Hashage MDP | Bcrypt via  PasswordEncoder | Test  passwordEncodingTest |
| JWT | HS512, 15 min TTL, refresh 7 j | JwtTokenProviderTest |
| Rôles | Stockés en BD, préfixés  ROLE\_ | IT + tests UI redirection |
| Limite brute-force | Bucket4j filter | RateLimitIT |

5. Statut des Tâches Au 17-06-2025

| ID | Tâche | Volet | Statut |
| --- | --- | --- | --- |
| A-01 | Journal d’audit + UI | Audit | ✅ |
| A-02 | Intégrité log (hash + sig) | Audit | ✅ |
| A-03 | RSA clé publique API | Audit | ✅ |
| A-04 | Vote chiffré client | Audit | ✅ |
| A-05 | Auth JWT & refresh | AuthN | ✅ |
| A-06 | Routes protégées rôles | AuthZ | ✅ |
| A-07 | Page scrutateur / admin résultats | Audit/AuthZ | ✅ |
| A-08 | Import CSV électeurs | AuthZ | 🔄 Spécifié (impl. Sprint Beta) |

6. Actions Futures

1. Finir import CSV électeurs (mots de passe temporaires, flag *mustChangePwd*).
2. CSP & Security-Headers middleware.
3. Docs Swagger + tests d’API contractuels.