📋 Spécification des Exigences Fonctionnelles & Non Fonctionnelles KYC

1. Introduction

Ce document formalise les exigences du système KYC, en distinguant besoins fonctionnels et non fonctionnels, avec un focus sur les interactions et contraintes côté système. Chaque exigence est accompagnée d'une description détaillée, d'actions à effectuer et de scénarios d'usage.

---

2. Exigences Fonctionnelles

2.1 Création et gestion du client

2.1.1 Préenregistrement et Saisie

Le système doit permettre la saisie, la modification et l'import automatique des données clients (particulier/entreprise) via une interface web ou INTRA.

Actions à effectuer :

- Générer un identifiant unique pour chaque nouveau client.
- Enregistrer toutes les données saisies dans la base de données.
- Contrôler l'unicité des informations critiques (ex : numéro CNI, NIU).
- Journaliser chaque opération de création ou modification.

Scénario nominal :

1. L'utilisateur accède au formulaire de création client.
2. Il saisit toutes les informations requises.
3. Le système contrôle l'unicité et la complétude.
4. Un identifiant unique est généré et affiché.
5. Les données sont enregistrées et l'opération journalisée.

Scénarios alternatifs :

- 2a. Si une information obligatoire est manquante, le système bloque la validation et affiche un message d'erreur.
- 3a. Si un doublon est détecté (CNI déjà existante), le système bloque la création et notifie l'utilisateur.

2.1.2 Signature électronique

Le système doit intégrer un dispositif de signature électronique (ePad) et assurer le stockage sécurisé des signatures (bitmap, vecteur, biométrie).

Actions à effectuer :

- Afficher le document à signer sur l'ePad.

- Capturer la signature et les métadonnées (pression, horodatage).
- Stocker le document signé dans le CBS et le journal d'audit.
- Permettre la consultation de la signature dans l'historique client.

Scénario nominal :

1. Le gestionnaire lance la procédure de signature.
2. Le client signe sur l'ePad.
3. Le système capture la signature et l'associe au dossier.
4. Le document signé est archivé et consultable.

Scénarios alternatifs :

- 2a. Si la signature est incomplète ou refusée, le système bloque la validation et affiche une alerte.
- 3a. Si l'ePad n'est pas détecté, le système propose une alternative ou signale l'incident.

2.1.3 Génération de documents

Le système doit générer automatiquement les fiches KYC, conventions et cartons de signature à partir des données validées.

Actions à effectuer :

- Remplir les modèles de documents avec les données du client.
- Générer les fichiers au format PDF.
- Bloquer la génération si des données ou documents obligatoires sont manquants.
- Archiver chaque document généré et l'associer au dossier client.

Scénario nominal :

1. Le gestionnaire valide le dossier client.
2. Le système génère automatiquement les documents nécessaires.
3. Les documents sont archivés et disponibles pour consultation ou impression.

Scénarios alternatifs :

- 2a. Si une donnée obligatoire est manquante, le système bloque la génération et affiche la liste des éléments à compléter.
- 3a. Si l'archivage échoue, une alerte est envoyée à l'administrateur.

2.1.4 Gestion des mandataires et actionnaires

Le système doit permettre l'ajout, la modification, la suppression, la consultation et l'export des mandataires et actionnaires via INTRA.

Actions à effectuer :

- Lier chaque mandataire/actionnaire au client principal.
- Vérifier les droits d'accès et d'édition selon le profil utilisateur.
- Exporter la liste des mandataires/actionnaires au format PDF ou Excel.
- Journaliser toutes les opérations et conserver l'historique.

Scénario nominal :

1. Le gestionnaire accède à la fiche client.
2. Il ajoute/modifie/supprime un mandataire ou actionnaire.
3. Le système vérifie les droits et enregistre l'opération.
4. L'historique est mis à jour et consultable.

Scénarios alternatifs :

- 2a. Si un champ obligatoire est manquant, le système bloque la validation.
- 3a. Si l'export échoue, une alerte est affichée et journalisée.

2.1.5 Gestion du matricule et référentiel

Le système doit générer automatiquement un matricule unique, contrôler l'unicité et historiser les modifications. Il doit permettre la gestion dynamique des référentiels (professions, statuts, etc.).

Actions à effectuer :

- Générer un matricule selon l'algorithme défini.
- Vérifier l'absence de collision avec les matricules existants.
- Historiser toute modification du référentiel.
- Appliquer immédiatement les changements dans les interfaces utilisateurs.

Scénario nominal :

1. Le gestionnaire crée ou modifie un client.
2. Le système génère ou met à jour le matricule.
3. Toute modification est historisée et visible dans l'historique du client.

Scénarios alternatifs :

- 2a. Si une collision est détectée, le système bloque l'opération et propose une intervention manuelle.
- 3a. Si une modification référentielle impacte des dossiers actifs, le système bloque la désactivation et notifie l'utilisateur.

2.1.6 Déclaration matrimoniale

Le système doit permettre la saisie, la validation et la gestion des justificatifs du système et du régime matrimonial.

Actions à effectuer :

- Proposer dynamiquement les options (monogamie, polygamie, communauté, séparation).
- Vérifier la présence et la validité des justificatifs joints.
- Bloquer la validation si aucune option n'est sélectionnée ou si le justificatif est invalide.
- Journaliser chaque action liée à l'état matrimonial.

Scénario nominal :

1. Le gestionnaire accède à la section état civil du client.
2. Il sélectionne le système/régime matrimonial et joint les justificatifs.

3. Le système valide et enregistre l'information.

Scénarios alternatifs :

- 2a. Si aucune option n'est sélectionnée, le système bloque la validation.
- 3a. Si le justificatif est invalide, le système refuse l'ajout et affiche un message d'erreur.

2.2 Gestion des comptes

2.2.1 Création et clôture de compte

Le système doit intégrer le CBS via API SOAP/REST pour la création et la clôture des comptes, générer le RIB et notifier automatiquement le client.

Actions à effectuer :

- Envoyer une requête API au CBS avec les données client validées.
- Recevoir et enregistrer les identifiants de compte et le RIB.
- Notifier le gestionnaire et/ou le client par email/SMS.
- Journaliser toutes les opérations de création et de clôture.

Scénario nominal :

1. Le gestionnaire valide la création d'un compte.
2. Le système envoie la demande au CBS.
3. Le CBS retourne le numéro de compte et le RIB.
4. Le système notifie le gestionnaire et journalise l'opération.

Scénarios alternatifs :

- 2a. Si le CBS ne répond pas, le système affiche une alerte et propose une relance.
- 3a. Si le RIB n'est pas généré, l'opération est bloquée et journalisée.

2.3 Contrôles identité et conformité

2.3.1 Validation documentaire

Le système doit contrôler automatiquement l'authenticité, le format et la date d'expiration des documents, avec escalade manuelle si besoin.

Actions à effectuer :

- Vérifier le format et le checksum de chaque document soumis.
- Comparer la date d'expiration à la date courante.
- Bloquer l'enregistrement si un document est invalide.
- Escalader le dossier à un gestionnaire pour validation manuelle si nécessaire.

Scénario nominal :

1. Le gestionnaire ou le client soumet un document.

2. Le système vérifie automatiquement l'authenticité et la validité.
3. Si tout est conforme, le document est accepté et journalisé.

Scénarios alternatifs :

- 2a. Si le format est incorrect, le système refuse le document et affiche un message d'erreur.
- 3a. Si la date d'expiration est dépassée, le système bloque l'enregistrement.

2.3.2 Contrôle de complétude

Le système doit vérifier automatiquement la complétude des dossiers selon le type de compte et alerter l'utilisateur en cas de manquant.

Actions à effectuer :

- Comparer les documents soumis à la liste obligatoire du référentiel.
- Générer une alerte ou un message d'erreur si des éléments sont manquants.
- Empêcher la validation finale tant que le dossier n'est pas complet.

Scénario nominal :

1. L'utilisateur soumet tous les documents requis.
2. Le système compare la liste et valide la complétude.
3. Le dossier passe à l'étape suivante du workflow.

Scénarios alternatifs :

- 2a. Si un document est manquant, le système bloque la validation et affiche la liste des pièces à fournir.

2.3.3 Détection doublons, blacklist, PPE, FATCA

Le système doit générer une clé unique pour chaque client, interroger les bases externes (blacklist, PPE, FATCA) et escalader automatiquement les cas positifs.

Actions à effectuer :

- Générer et comparer la clé unique avec les enregistrements existants.
- Interroger les bases de données externes pour blacklist, PPE, FATCA.
- Bloquer ou escalader le dossier en cas de correspondance.
- Journaliser toutes les vérifications et alertes.

Scénario nominal :

1. Le système génère la clé unique à la création du client.
2. Il interroge les bases externes et valide l'absence de correspondance.
3. Le dossier poursuit son traitement normal.

Scénarios alternatifs :

- 2a. Si un doublon est détecté, le système bloque la création et notifie l'utilisateur.
- 3a. Si le client est sur une blacklist, le dossier est bloqué et une alerte conformité est générée.

2.4 Blocage/Déblocage

Le système doit permettre le blocage ou le déblocage automatique des comptes ou clients, notifier les parties prenantes et journaliser l'opération.

Actions à effectuer :

- Identifier tous les comptes liés au client.
- Appliquer le statut « Bloqué » ou « Débloqué » selon la décision.
- Notifier les parties prenantes par email/SMS.
- Enregistrer l'opération dans le journal d'audit.

Scénario nominal :

1. L'analyste conformité décide de bloquer un client.
2. Le système applique le statut « Bloqué » à tous les comptes liés.
3. Les parties prenantes sont notifiées et l'opération est journalisée.

Scénarios alternatifs :

- 2a. Si un compte est déjà bloqué, le système affiche une alerte et ne modifie pas le statut.
- 3a. Si la notification échoue, une alerte technique est générée.

2.5 Workflow, reporting & audit

Le système doit permettre la configuration dynamique des workflows, proposer un moteur graphique, une bibliothèque de contrôles, le reporting temps réel et un audit trail inviolable.

Actions à effectuer :

- Créer, modifier et activer des workflows via une interface graphique.
- Séquencer et paralléliser les étapes de validation.
- Générer et exporter des rapports d'activité et de rejet.
- Journaliser toutes les actions critiques dans un audit trail sécurisé.

Scénario nominal :

1. L'administrateur configure un nouveau workflow via l'interface graphique.
2. Le système applique la configuration et l'active.
3. Les utilisateurs suivent le nouveau parcours de validation.

Scénarios alternatifs :

- 2a. Si une étape du workflow est mal configurée, le système bloque l'activation et affiche un message d'erreur.
- 3a. Si l'export de rapport échoue, une alerte est générée.

2.6 Gestion documentaire

Le système doit assurer la classification, l'archivage, le versioning et l'indexation automatique des documents, selon un plan de classement structuré.

Actions à effectuer :

- Classer automatiquement les documents selon le type de client et le plan de classement.
- Générer des codes de classification et d'archivage.
- Versionner chaque document et conserver l'historique.
- Permettre la recherche rapide et l'accès à l'historique documentaire.

Scénario nominal :

1. Un document est ajouté ou modifié dans le dossier client.
2. Le système classe, archive et versionne automatiquement le document.
3. L'historique est consultable à tout moment.

Scénarios alternatifs :

- 2a. Si le classement échoue, le système affiche une alerte et journalise l'incident.
- 3a. Si une version est supprimée par erreur, le système permet la restauration.

---

3. Exigences Non Fonctionnelles

Pour chaque exigence non fonctionnelle, des scénarios de test et d'incident peuvent être définis sur demande.

Document validé le 17/06/2025 – version narrative structurée, chaque exigence accompagnée d'actions détaillées et de scénarios d'usage.