Titre du document

Tâche 3.7 Système d'archivage sécurisé des documents dématérialisés

Livrable : Tâche 3.7.2

Architecture du système d'archivage et de restauration

Objet du document

L'archivage numérique des documents électroniques s'impose progressivement à la filière logistique et transport aussi bien pour les transactions douanières, les transactions commerciales (commandes, facturations) et l'exécution-même des fonctions opérationnelles.

Le présent document décrit l'architecture de l'espace de stockage sécurisé Pass'IN qui sera mis à disposition des utilisateurs du projet Noscifel.

Informations sur le document

Responsable	Référence	Description	Date livraison
CHONOSERVICES	T3.7.2	Version 1.0	28/03/2014
CHONOSERVICES	T3.7.2	Version 1.1	24/09/2014
CHONOSERVICES	T3.7.2	Version 1.2	22/10/2014

Contributions

Contributeurs	Pourcentage
CHONOSERVICES Connaissances antérieures	100 %

Table des matières

1 Présentation générale

Le présent document décrit l'architecture fonctionnelle de l'espace électronique sécurisé qui sera mis à disposition des utilisateurs du projet Noscifel.

Cet espace électronique est sécurisé sur des serveurs cryptés sécurisés au sein d'un site classé PS1 et certifié Opérateur d'Importance Vitale (O.I.V.).

Véritable espace électronique sécurisé de confiance, l'espace de stockage sécurisé de l'Imprimerie Nationale stocke des documents électroniques sensibles et permet :

- L'authentification des accès aux données
- La confidentialité des données
- La préservation de la valeur probante des originaux électroniques
- L'assurance de l'intégrité des documents stockés
- L'horodatage et la traçabilité
- L'accompagnement des télé-procédures
- La gestion du contenu par le détenteur du coffre-fort

Les bénéfices de cette solution :

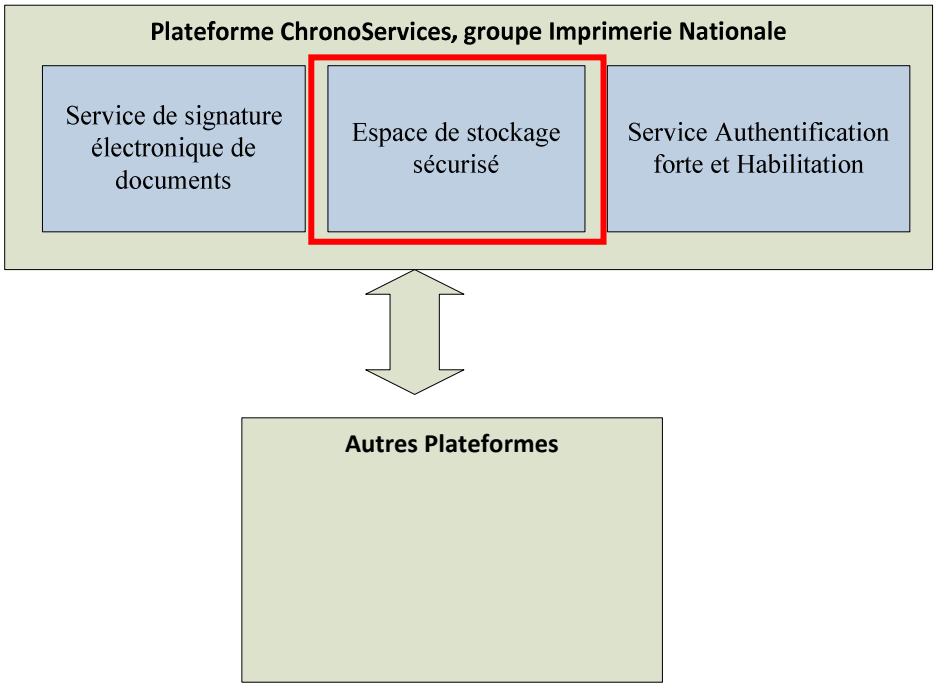
- Mutualisation de l'espace O.I.V. et des infrastructures sécurisées
- Environnement de confiance : environnement sécurisé et confidentiel, pérennité de l'infrastructure, opérateur de confiance du secteur public
- Gestion et la rationalisation des politiques d'archivage, des politiques de sécurité et la garantie de la confidentialité
- Facilitation des premiers services : consultations, extractions et copies certifiées.

Cet espace électronique sécurisé respecte les normes suivantes :

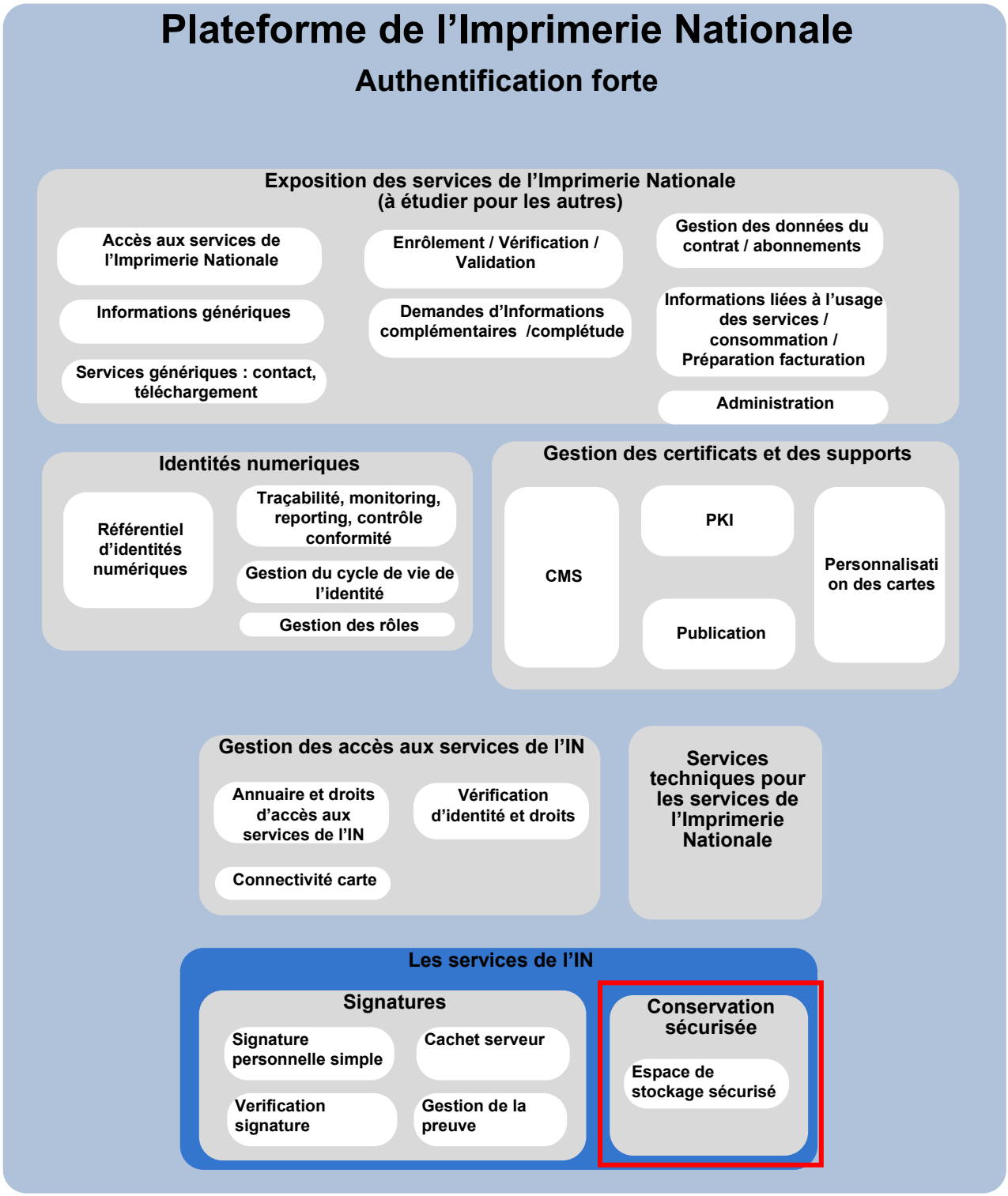
- La norme NF Z42-013 : Archivage électronique - Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes (publiée en mars 2009),
- La norme NF Z42-020 : Spécifications relatives au composant Coffre-Fort Numérique destiné à la conservation d'informations numériques dans des conditions de nature à garantir leur intégrité dans le temps,
- la norme ISO 14721 : Archivage électronique – Partie 1 : Spécifications relatives à la conception et au fonctionnement d'un système d'informations pour la conservation d'informations électroniques (OAIS)

2 Architecture fonctionnelle et technique de la plateforme de l'Imprimerie Nationale pour le projet Noscifel

2.1 Architecture général



2.2 Architecture fonctionnelle de la plateforme Pass'IN

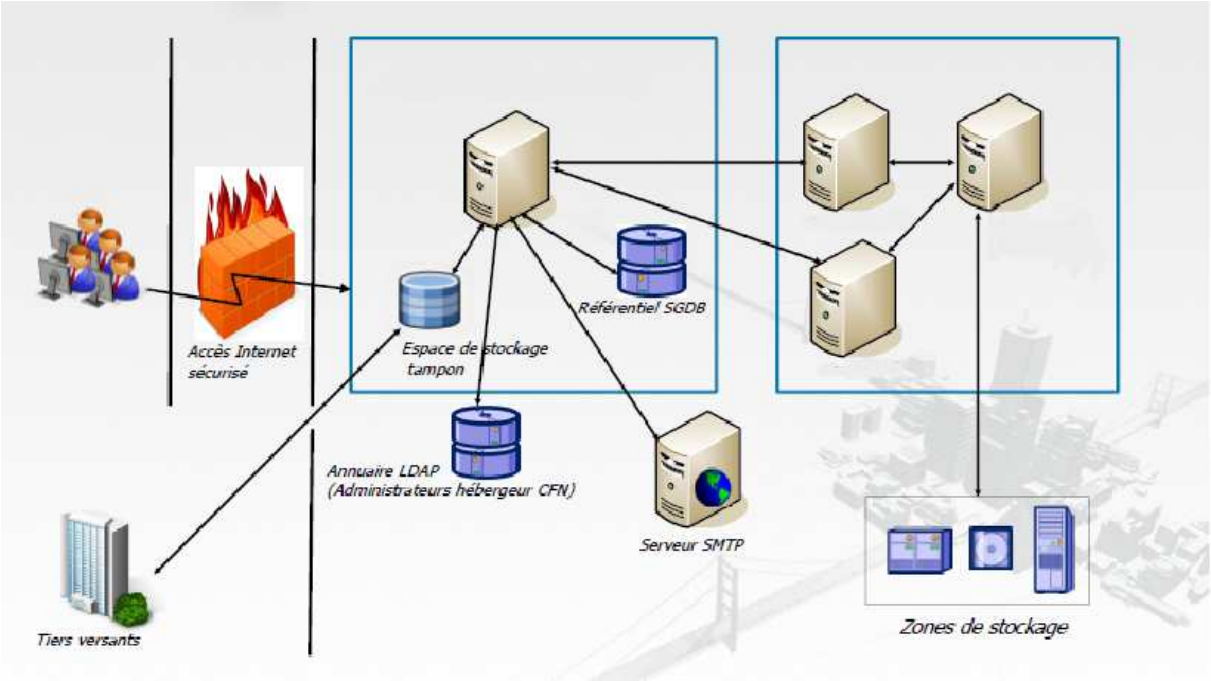


2.1 Qualité des matériels, équipements et progiciels

Les exigences générales sont couvertes par les mesures suivantes :

- **Des infrastructures et un environnement** sécurisé, confidentiel et pérenne.
- **Administrabilité** : Le composant dispose de ses propres moyens d'administration au travers de fonctions spécifiques proposées par les progiciels utilisés.
- **Maintenabilité** : Pour assurer l'exploitation, le maintien en conditions opérationnelle du système.
- **La gestion et la rationalisation** de la politique d'archivage, des politiques de sécurité et la garantie de la confidentialité.
- **Archivage des données en France afin d'être conforme à la volonté de la CNIL.**
- **Protéger les sites d'hébergement contre les intrusions physiques et logiques**

2.2 Architecture technique de l'espace de stockage sécurisé



2.1 Architecture fonctionnelle du logiciel d'archivage

- Agent d'archivage

On distingue au niveau des fonctions d'archivage deux types d'agents différents : des agents d'interface avec des applications et des agents d'interface avec les utilisateurs.

Un agent Application permettra d'archiver tous les objets spécifiques à une application (fichiers, lignes d'une table d'un SGBDR, …) quand à l'agent utilisateur il présente à la fois des fonctions d'administration et des fonctions d'archivage manuel initié par l'utilisateur.

- Moteur d'archivage

Ce moteur fonctionne en liaison avec un espace temporaire de stockage à partir duquel les objets à archiver peuvent transiter soit en provenance d'un agent soit par dépôt direct dans un espace.

- Les connecteurs

Il s'agit d'agents d'application spécialisés pour des domaines particuliers. A ce jour, il existe un connecteur SAP et deux connecteurs de messagerie, l'un pour Lotus Notes, l'autre pour Exchange (redevance logicielle complémentaire).

Ils permettent à ces applications de mettre en œuvre de manière transparente pour les utilisateurs des fonctions d'archivage standard (cas SAP) ou des fonctions d'archivage additionnelles (cas des messageries).

Il est important de noter que le logiciel met en œuvre des interfaces génériques avec des composants périphériques.

- Les API

Les API peuvent être utilisées en complément des commandes ou fonctionnalités standards disponibles sur le produit.

Les API Java de l'agent Application sont généralement localisées sur la même machine que les connecteurs. Ces API vont permettre de réaliser des prétraitements sur les objets issus des applications afin de modifier, compléter le comportement du produit. Ainsi, il est possible par exemple grâce à ces interfaces, d'extraire automatiquement des valeurs de métadonnées d'un objet applicatif ayant un format spécifique ;

Les API permettent de réaliser par programmation des actions accomplies par interface Web et les connecteurs standards, allant de la création de lots et d'objets, à la création et au suivi d'archivage et de restitutions.

- Gestion de la sécurité

Les accès au service sont effectués dans un contexte de session utilisateur, ce qui implique l'utilisation de service d'authentification et de gestion d'habilitation.

Ces services externes d'authentification et d'habilitation seront accédées par l'intermédiare d'interfaces disponibles en standard sur la plateforme Java, à savoir JAAS pour l'authentification et JNDI pour l'accès aux habilitations (au travers de services d'annuaires).

Quand la personne est authentifiée sur la plateforme Noscifel, l'affichage du portail et des services de l'IN se fera grâce aux mécanismes de :

- d'iframe : (dans l'IHM Noscifel on voit le service de l'IN) ou
- d'ouverture dans une autre fenêtre

Il sera nécessaire de réaliser la vérification des droits d'accès au service de la personne (dans un « active directory ») cela sera réalisé à l'aide de Web SSO qui renverra l'information d'accès au service.

3 Présentation générale de l'espace de stockage sécurisé Pass'IN

Dans le cadre de son activité, une société peut être amenée à archiver des documents de différentes sortes (contrats, factures, bulletins de salaires,..) à destination de ses clients ou de ses salariés. L'utilisateur final peut déposer et consulter des documents (éventuellement déposés par un tiers), de manière sécurisée, et intuitive via un simple accès réseau.

L'utilisateur peut également pouvoir rechercher et sélectionner les documents qu'il veut consulter.

L'espace de stockage sécurisé permet de déposer un document dans son espace personnel. Ce document sera ensuite disponible via un accès réseau.

3.1 Notions et fonctionnalités

- Salle des coffres

La salle des coffres, créée par un administrateur, contient un ensemble de coffres. Le volume des coffres (ou espaces de stockage) est paramétrable.

- Coffre

Un coffre est un « dossier » de la salle des coffres. Il contient un ensemble de documents et détermine l'indexation utilisée pour y accéder.

- Partage

Le propriétaire de la salle des coffres donne les droits d'accès à un ou plusieurs de ses coffres pour un ou plusieurs utilisateurs.

- Document

Un document désigne le plus petit objet numérique que l'on puisse manipuler à l'intérieur de l'espace de stockage sécurisé.

- Indexation

L'indexation correspond à l'ensemble des éléments utilisés pour référencer un document dans l'espace de stockage sécurisé. L'indexation détermine la manière de rechercher un document.

- Tag / mot clés

Un tag est un élément d'indexation, il s'agit d'un terme associé à un document qui permet sa recherche ultérieure. Les tags sont choisis au moment du dépôt d'un document.

Un document peut avoir plusieurs tags.

- Dépôt

L'opération de dépôt consiste à ajouter un document.

L'utilisateur peut déposer ses documents depuis son navigateur web.

- Copie

L'opération de copie consiste à récupérer une image intègre d'un document déposé.

- Consultation

L'opération de consultation consiste à visualiser un document. La consultation ne détruit pas le document dans le coffre.

- Destruction

L'opération de destruction consiste à effacer un document d'un coffre. Seul le propriétaire d'un coffre dispose de fonctionnalités permettant de détruire un document dans le coffre.

- Recherche

L'utilisateur peut rechercher des documents sur les coffres pour lesquels il a été habilité au moins à l'opération de consultation. La recherche suit des critères généraux (nom du document, date, taille) ou d'indexation.

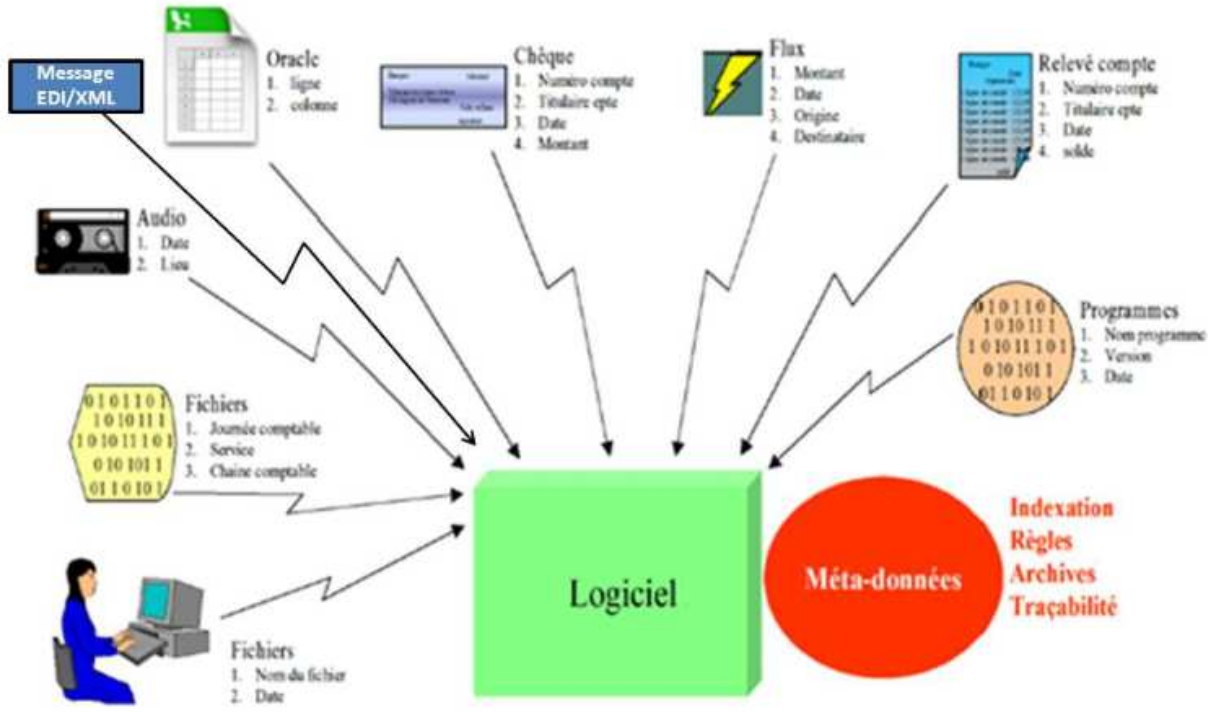
La recherche peut se faire sur un ou sur l'ensemble des coffres autorisés de la salle des coffres.

- Télécharger

L'utilisateur peut visualiser et/ou récupérer une copie d'un document déposé, directement depuis son navigateur web.

- Notion d'objets

La diversité des problématiques d'archivage nous a amené à proposer une plate-forme qui soit capable d'archiver aussi bien des images que des documents, aussi bien des fichiers que des tables relationnelles ou le résultat d'une requête. La notion d'objet à ainsi été adoptée. Le produit à la capacité d'adresser des structures quelconques (suite de 0 et de1). A chacun de ces objets sont associés des métadonnées, complètement dépendantes des métiers, à partir desquelles les recherches ultérieures seront opérées. Il n'y a aucune limitation quant aux types d'objets admissibles, aux types de formats utilisés, aux environnements desquels ces objets sont issus.



3.2 Les différents acteurs

Les tableaux suivants présentent les différents acteurs intervenants sur l'espace de stockage sécurisé en précisant succinctement leurs rôles.

Acteurs	Description
Propriétaire	L'utilisateur propriétaire est l'acteur principal de l'application, il peut déposer, rechercher, supprimer ou récupérer des documents déposés par ou pour lui. Le propriétaire est le seul à pouvoir gérer les droits d'accès et la suppression des documents.
Copropriétaire	Le copropriétaire est un utilisateur possédant les mêmes droits d'accès que le propriétaire mise à part celui de supprimer des droits à un utilisateur mandataire.
Mandataire	L'utilisateur mandataire est autorisé par le propriétaire à accéder à un ou plusieurs coffres pour déposer et/ou récupérer des documents. Il dispose de différents niveaux d'habilitations selon les droits qui lui ont été donnés (dépôt/consultation ou consultation uniquement). On utilise le terme de copropriétaire pour un utilisateur disposant de droits étendus : un copropriétaire de salle des coffres dispose de toutes les fonctionnalités de l'espace de stockage sécurisé en dehors de la suppression des documents et de la gestion des droits d'accès.

Acteurs	Description
Administrateur **L'Imprimerie Nationale**	L'administrateur est chargé d'administrer les compagnies clientes Il est en charge de gérer la capacité de stockage, les fonctionnalités accessibles de chaque compagnie. Il gère les managers de chacune de ses compagnies. Il a accès aux journaux des activités de l'espace de stockage sécurisé.

Les acteurs

Identification des acteurs

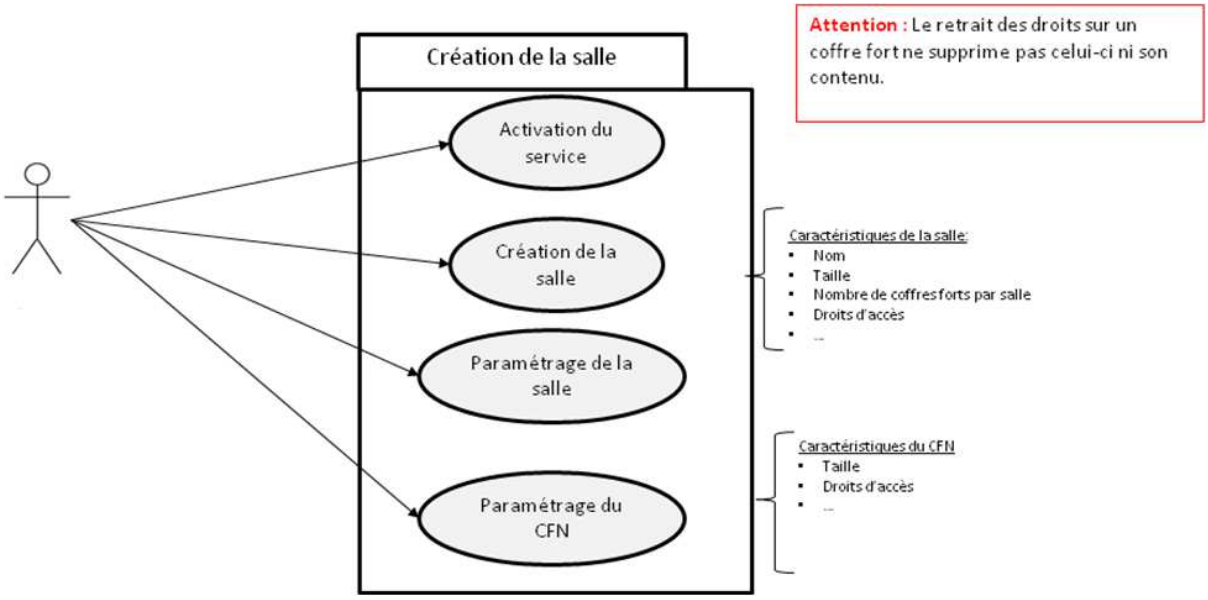
Pour le système, la couverture des risques nécessite la mise en place des éléments suivants :

- Procéder à l'authentification forte de tous les acteurs (administrateurs et utilisateurs)
- Au minimum, procéder à l'authentification par identifiant / mot de passe.
- Utiliser un annuaire LDAP centralisé pour l'identification et l'authentification des acteurs.

3.3 L'espace de stockage sécurisé comporte deux interfaces

3.3.1 L'interface d'administration de l'Imprimerie Nationale

L'interface d'administration permet à l'Imprimerie Nationale la gestion des compagnies, des acteurs, cette interface propose les fonctionnalités suivantes :



- La gestion des compagnies
- La gestion des utilisateurs :
  - Ajout d'un utilisateur ;

○ Recherche d'un utilisateur ;

○ Désactivation d'un utilisateur ;

○ Accès aux caractéristiques du compte (volumétrie, droits d'accès reçus pour chaque salle des coffres dont l'utilisateur a accès).

- La gestion des salles des coffres d'un utilisateur :

  ○ Accès aux caractéristiques de la salle des coffres (volumétrie, droits d'accès donnés).

- La gestion des offres commerciales :

  ○ Ajout d'une offre commerciale ;

  ○ Désactivation d'une offre commerciale (si l'espace de stockage liés à cette offre est nul) ;

  ○ Accès aux caractéristiques de l'offre (liste des salles des coffres).

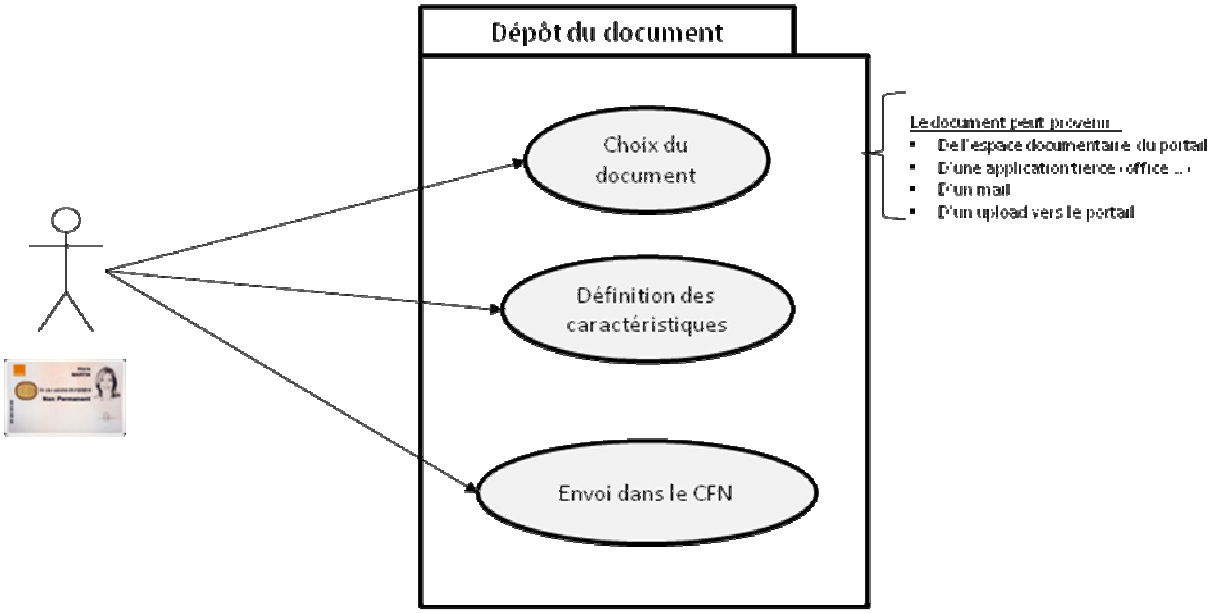
- Le suivi de l'activité (journal)

3.3.2 Interface utilisateur

Interface utilisateur (propriétaire, copropriétaire, mandataire) permet :

- L'accès à une aide en ligne
- Le dépôt du document
  - Directement depuis son navigateur Web
  - Dans une zone de dépôt spécifique (poste restante)

    Une société ou un tiers peut déposer des documents dans une zone de dépôt spécifique de l'intéressé (un utilisateur du système).
    Les documents restent en poste restante tant qu'ils n'ont pas été déplacés par l'utilisateur dans un de ses coffres.
  - Par un injecteur paramétrable (développement spécifique hors projet Noscifel)
  - Par e-mail
  - Possibilité de signer les données pour authentifier le dépositaire (avec carte à puce d'authentification)



- La recherche avancée
  - Par coffre ou sur l'ensemble des coffres
  - Par critères de dates ou d'indexation

- La récupération d'une copie d'un document archivé, directement depuis son navigateur web