

UNIVERSITÉ DE YAOUNDÉ I  
ECOLE NATIONALE SUPÉRIEURE  
POLYTECHNIQUE  
DÉPARTEMENT DU GÉNIE  
INFORMATIQUE

UNIVERSITY OF YAOUNDE I  
NATIONAL ADVANCED SCHOOL OF  
ENGINEERING  
DEPARTEMENT OF COMPUTER  
SCIENCE



Mémoire de fin d'étude/Master of Engineering

---

---

Présenté et soutenu le *18 juillet 2017* par :  
**FOKAM POKA ARSENE**

---

**SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN  
CLOUD**

---

---

En vue de l'obtention du  
**DIPLOME D'INGENIEUR EN CONCEPTION EN GÉNIE INFORMATIQUE**  
Sous la direction de :  
Dr MANI ONANA Serge Flavien

**MEMBRES DU JURY**

PRÉSIDENT DU JURY	Pr. PETTANG Chrispin
EXAMINATEUR	Dr CHANA Anne Marie
RAPPORTEURS	Dr MANI ONANA Serge Flavien Dr NANA MBINKEU Rodrigue Carlos
INVITÉ	M. YANGOUA Marien, Chef Service Informatique Centre Pasteur Du Cameroun

## Dédicace

---

Que toute ma famille, et singulièrement mes parents  
**POKA Siméon** et **KENGNE Jeannette** trouvent dans ce  
travail un motif de saine fierté pour le rôle spécial qu'elle a joué  
et continue de jouer dans ma modeste vie.

## Remerciements

---

Parce que le présent mémoire est le fruit d'une contribution plurielle et substantielle, je tiens ici à exprimer toute ma gratitude d'abord à l'ETERNEL le DIEU CREATEUR, source de toute chose, à l'égard de qui toute la création raisonnable doit, par humilité, reconnaissance ; ensuite :

- ✎ Au Président du Jury **Pr PETTANG Chrispin Claude** qui de loin, m'inspire la grandeur, et de prêt, m'encourage à l'excellence dans le travail ;
- ✎ A **Dr MANI ONANA Serge Flavien**, qui a été pour moi une lumière sur le sentier de ce travail et auprès de qui j'ai eu l'honneur de goûter au fruit que peut produire la conciliation entre la grandeur et la modestie, la densité intellectuelle et la simplicité sociale ;
- ✎ A **Dr NANA MBINKEU Rodrigue Carlos**, pour le privilège qu'il m'offre d'être rapporteur et de me suivre méticuleusement dans mon travail ;
- ✎ A **Dr CHANA Anne Marie** dont, l'ensemble formé par l'extraordinaire finesse d'analyse scientifique et le constant zèle qu'on peut admirer chez elle m'a propulsé dans la conquête de la connaissance tout au long de ma formation ;
- ✎ A mon encadreur professionnel **YANGOUA Marien** pour m'avoir chaleureusement accueilli au sein de sa section, pour sa disponibilité, les ressources matérielles, et l'accompagnement qu'il m'a manifesté alors que je faisais mes premiers pas dans le milieu professionnel ;
- ✎ A tout le personnel de la cellule informatique du Centre Pasteur du Cameroun, pour leur accueil chaleureux ;
- ✎ A ma sœur et complice **SIMO MBOUYIM Aurélia** grâce au support moral de laquelle les difficultés socio-professionnelles inhérentes à notre foi commune en l'ETERNEL, ont été sereinement surmontées ;
- ✎ A mon grand frère **Dr KAMTA Médard Elvice** qui m'a témoigné un appui particulier tout au long de ma formation par ses prières, ses conseils, son suivi ;
- ✎ A mon mentor **AINAM Jean Paul** dont l'hospitalité manifestée du premier au 03 juillet 2017 dans le campus de l'Université Adventiste COSENDAL m'a permis de réviser profondément mon travail technique ;
- ✎ A mon camarade ingénieur **NGNAWE Jonas** pour les nuits blanches passées ensemble dans les efforts incessants.

Le quotidien des entreprises le prouve on ne peut plus fortement : la préservation des données est une pratique d'entreprise vitale. L'archivage des données d'entreprise doit donc se faire conformément aux exigences réglementaires. Elle nécessite la conservation des copies de sécurité des fichiers tout en réduisant la charge qui pèse sur le stockage primaire et en libérant des ressources pouvant dès lors être consacrées à des tâches opérationnelles. Grâce à l'avènement des services Cloud, il est devenu possible d'archiver des données en éliminant investissement initial et bien de dépenses subséquentes. Malheureusement cette sous-traitance cloud pose le problème de sécurité. En effet, quand bien même certains SAE-Cloud offrent la possibilité de chiffrer les sauvegardes, la sécurité n'est pas suffisamment garantie dans la mesure où le chiffrement est assuré par le prestataire cloud qui partage dès lors la confidentialité du document avec le client.

Ce mémoire propose une révision de l'approche habituelle d'archivage électronique en Cloud en insistant sur la mise en œuvre d'une politique de sécurité interne des sauvegardes. Cette politique consiste en un mot, à chiffrer d'abord chaque sauvegarde, les rassembler avant de les stocker dans le Cloud. La mise en œuvre de ce Système Cryptographique pour Archivage Electronique(SCAE) est basée sur UML pour sa modélisation et les frameworks Symfony et Bootstrap pour son implémentation.

Dotée de cet outil, toute entreprise peut continuer à consulter librement ses documents archivés en ayant l'assurance que ses données sensibles demeurent aussi confidentielles quoique stockées à distance.

**Mots clés :** archivage, cloud, cryptographie, SCAE

# Abstract

---

The everyday life of companies proves it : the preservation of data is a vital business practice. The archiving of business data must therefore be done in accordance with regulatory requirements. It requires the retention of backup copies of files while reducing the burden on primary storage and freeing up resources that can be used for operational tasks. With the advent of cloud services, it became possible to archive data by eliminating initial investment and many subsequent expenses. Unfortunately, this cloud outsourcing poses a security problem. Indeed, even if some EAS-Cloud offers the possibility of encrypting backups, security is not sufficiently guaranteed since the encryption is ensured by the cloud provider, which then shares the confidentiality of the document with the client.

This dissertation proposes a revision of the usual approach of electronic archiving in Cloud by insisting on the implementation of a security policy of internal safeguards. This policy simply consists in encrypting each backup first, gathering them before storing them in the Cloud. The implementation of this Cryptographic Electronic Archiving System (CEAS) is based on UML for its modelling and the Symphony and Bootstrap frameworks for its implementation.

With this tool, any company can continue to freely consult its archived documents with the assurance that its sensitive data remains confidential, even though stored remotely.

**Keywords :** archiving, cloud, cryptography, EAS, CEAS

# Table des matières

---

<b>Introduction Générale</b>	<b>1</b>
<b>1 DEFINITION DES CONCEPTS THEORIQUES ET PROBLEMATIQUE</b>	<b>4</b>
1.1 Vocabulaire de l'archivage . . . . .	5
1.2 Vocabulaire du Cloud . . . . .	6
1.3 Vocabulaire de la cryptographie . . . . .	7
1.4 Problématique . . . . .	8
<b>2 ETAT DE L'ART</b>	<b>10</b>
2.1 Types d'approches d'archivage cloud . . . . .	11
2.2 Présentation des catégories existantes d'archivage selon les approches de services Cloud . . . . .	12
2.3 Insuffisances sécuritaires des catégories existantes d'archivage selon les approches de services Cloud . . . . .	16
<b>3 METHODOLOGIE</b>	<b>18</b>
3.1 Description de SCAE-CPC . . . . .	18
3.2 Expression des besoins analyse et conception . . . . .	24
<b>4 IMPLÉMENTATION ET RÉSULTATS</b>	<b>41</b>
4.1 Choix des outils . . . . .	42
4.2 Implémentation . . . . .	45

**SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD**

4.3 Résultats . . . . .	47
<b>Conclusion</b>	<b>56</b>
<b>REFERENCE</b>	<b>57</b>

## Table des figures

---

1.1	Principe du chiffrement symétrique . . . . .	8
1.2	Principe du chiffrement asymétrique . . . . .	8
2.1	Description de différentes formes de SAE en fonctions de la répartition des services entre l'entreprise et le fournisseur de service Cloud . . . . .	17
3.1	Illustration de la forme de SAE mise en œuvre dans SCAE-CPC . . . . .	19
3.2	Principe de conservation des documents dans SAE-CPC . . . . .	23
3.3	Diagramme de cas d'utilisation . . . . .	25
3.4	Diagramme de séquences système de l'inscription d'un personnel . . . . .	28
3.5	Diagramme de séquences système de la sauvegarde d'un fichier . . . . .	30
3.6	Diagramme de séquences système de la recherche d'une archive . . . . .	33
3.7	Diagramme de séquences système de la consultation d'une archive . . . . .	34
3.8	Architecture de SCAE-CPC . . . . .	35
3.9	Diagramme de classes métiers de SCAE-CPC . . . . .	37
3.10	Modèle logique de données de SCAE-CPC . . . . .	38
3.11	Architecture technique . . . . .	39
4.1	Architecture MVC . . . . .	43
4.2	Diagrammes de packages . . . . .	46
4.3	Diagrammes de packages . . . . .	47
4.4	Page d'inscription de SCAE-CPC . . . . .	48



4.5	Page de connection de SCAE-CPC . . . . .	49
4.6	Liste des utilisateurs de SCAE-CPC . . . . .	50
4.7	Edition de role dans SCAE-CPC, cas de Jonas . . . . .	51
4.8	Création d'une nouvelle sauvegarde . . . . .	52
4.9	Liste des sauvegardes . . . . .	53
4.10	Archivage d'un document . . . . .	54
4.11	Archivage d'un document . . . . .	55

# ACRONYMES

---

<b>AUSCGIE</b>	<i>Acte uniforme relatif au droit des sociétés commerciales et du groupement d'intérêt économique</i>
<b>BD</b>	<i>Base de Données</i>
<b>CPC</b>	<i>Centre Pasteur du Cameroun</i>
<b>CPU</b>	<i>Central Processing Unit</i>
<b>DAO</b>	<i>Data Access Object</i>
<b>GSA</b>	<i>General Services Administration</i>
<b>FOS</b>	<i>Friends Of Symfony</i>
<b>GED</b>	<i>Gestion Electronique de Documents</i>
<b>IaaS</b>	<i>Infrastructure as a Service</i>
<b>IDE</b>	<i>Integrated Development Environment</i>
<b>KNP</b>	<i>KnplabsL</i>
<b>MVC</b>	<i>Model-View-Controller</i>
<b>ORM</b>	<i>Object-Relational Mapping</i>
<b>OS</b>	<i>Operating System</i>
<b>PaaS</b>	<i>Platform as a Service</i>
<b>Piaf</b>	<i>Portail International Archivistique Francophone</i>
<b>PHP</b>	<i>Hypertext Preprocessor</i>
<b>PUGX</b>	<i>PhpUserGroup X</i>
<b>RUP</b>	<i>Rational Unified Process</i>
<b>SaaS</b>	<i>Software as a Service</i>
<b>SAE</b>	<i>Système d'Archivage Electronique</i>
<b>SCAE</b>	<i>Système Cryptographique pour Archivage Electronique</i>
<b>SAE-Cloud</b>	<i>Système d'Archivage Electronique en Cloud</i>
<b>SCAE-CPC</b>	<i>Système Cryptographique pour Archivage Electronique du CPC</i>
<b>SGBD</b>	<i>Système de Gestion de Base de Données</i>
<b>UP</b>	<i>Unified Process</i>
<b>VPN</b>	<i>Virtual Private Network</i>

# Introduction Générale

---

Le passage du non connecté au tout connecté est une réalité technique et économique qui s'impose à tous. L'économie de service liée à la mutualisation des infrastructures et des logiciels sur Internet se développe pour permettre à chacun d'optimiser ses coûts et son temps tout en maîtrisant ses risques. A plusieurs reprises, les entreprises ont été amenées à faire des choix sur leur politique d'externalisation de leurs infrastructures et de leurs données. Les entreprises âgées se sont développées sans Internet. Elles ont cependant dû s'adapter pour rester compétitives en utilisant Internet comme moyen de communication et d'information. Les entreprises plus récentes se sont développées dans le contexte de l'Internet, ce qui leur a permis de créer de nouvelles activités et de nouveaux modes de communication et d'échange. Tous ces changements rapides ont donné lieu à une structuration des échanges et des services au travers des normes et règlements sectoriels. Les entreprises de demain utiliseront et se développeront nativement avec le Cloud. Ce dernier s'entend comme ensemble de ressources matérielles interconnectées gérées par un système d'exploitation capable de donner une vue unique à l'utilisateur. Cette évolution est inéluctable car elle est source d'économie et de compétitivité. L'offre est déjà fortement présente et les services fleurissent pour permettre de mettre en œuvre une économie numérique basée sur l'usage du Cloud. Les documents et les données des entreprises sont au cœur du système d'information et migrent déjà sur le Cloud. Ces informations représentent le patrimoine économique et stratégique des entreprises. Le classement, en vue de la pérennisation documents sous forme numérique, encore très internalisé ou externalisé d'une manière confidentielle, devra pouvoir s'intégrer dans cette nouvelle économie. L'importance des archives impose l'usage d'un support de stockage de l'information, assurant la sécurité mais surtout la pérennité de cette information. Or nous assistons à une évolution régulière des technologies ainsi que des supports de stockage d'informations, allant des ancêtres disquettes à l'actuel Cloud passant par la génération des CD. Au

regard du volume des archives, de leur l'importance croissante pour toute entreprise, ainsi que la sécurité de l'entreprise elle-même, on ne peut s'empêcher de se poser les questions suivantes :

- Pouvons-nous réellement sous-traiter l'archivage électronique des informations très souvent sensibles, en texte clair et parler de sécurité de l'entreprise ?
- Comment garantir simultanément la disponibilité des archives électroniques et la confidentialité de celles-ci ? Telles sont les questions constitutives de la problématique, auxquelles il sera question d'apporter une réponse tout au long de ce travail.

## **SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD**

Ce travail poursuit les objectifs suivants :

- Accompagner nos entreprises dans le processus de dématérialisation des archives, pour résoudre les problèmes liés à l'encombrement toujours plus grandissant inhérent au système d'archivage classique ;
- Garantir la confidentialité des archives électroniques ;
- Garantir l'intégrité et la pérennité des archives malgré le contexte d'évolution des supports de stockage d'information.

Dans les entreprises, les enjeux induits par l'archivage électronique sont multiples.

- Sur le plan stratégique, il existe tout d'abord un axe stratégique qui consiste à décider quelles données doivent être conservées, en dehors des aspects purement obligatoires. En effet, selon son domaine d'activité, il peut être intéressant pour une entreprise de conserver ses différents procédés ou savoir-faire, et ce afin de pouvoir les réutiliser ultérieurement ou tout simplement en garder une trace historique.
- Un second enjeu concerne l'aspect légal et le respect des lois en vigueur. Sur ce point, il s'agit avant tout pour une société de bien connaître ses obligations et l'étendue des sanctions en cas de non-respect de ces dernières.
- Par ailleurs, d'un point de vue organisationnel, une entreprise se doit d'optimiser la structuration de ses données afin d'en faciliter la gestion, de maîtriser la redondance de l'information et de détruire les données inutiles ou périmées qui alourdissent le système. Un autre élément est à prendre en compte : il ne faut pas oublier de favoriser l'accès à l'information des collaborateurs tout en respectant des droits d'accès établis de façon stricte.
- Quant à l'enjeu juridique, il concerne essentiellement les données conservées à des fins légales et se situe entre organisation et technique. Il est important pour une entreprise de vérifier qu'en cas de contentieux, par exemple, le système d'archivage électronique permettra de retrouver les pièces requises dans les délais impartis et que ces dernières, de plus, pourront être effectivement retenues comme éléments de preuve.

Afin de poursuivre le contexte de dématérialisation des données, notre approche d'archivage vise simplement à constituer, ensuite, chiffrer les sauvegardes et à sous-traiter leur stockage par un fournisseur de service Cloud. Pour décrire l'approche mise en œuvre, le mémoire est structuré en 5 chapitres à savoir :

- Chapitre 1 : Concepts théoriques qui présente les différents notions théoriques relatives à au Cloud Computing, à l'archivage électronique et à la cryptographie.
- Chapitre 2 : Etat de l'art qui dresse un état de l'art du Cloud relatif à l'archivage électronique. C'est une démarche préliminaire qui nous permettra de capitaliser les savoirs et les savoirs faire existants pour mener à bien ce projet. Ce chapitre se terminera par la justification du choix de notre solution.
- Chapitre 3 : Méthodologie qui décrit la méthodologie suivie et les approches retenues pour la mise en place du système cryptographique d'archivage électronique du Centre Pasteur du Cameroun (SCAE-CPC).

## **SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD**

- Chapitre 4 : Analyse et Conception qui s'étend du recueil des besoins effectuées auprès des utilisateurs à la présentation des premiers artefacts résultant de la conception de SCAE-CPC.
- Chapitre 4 : Implantation et Résultats. Dans ce chapitre nous présenterons dans un premier temps les outils utilisés pour mettre sur pied la conception que nous avons effectuée et nous décrivons les fonctionnalités produites par SCAE-CPC.

# 1

## DEFINITION DES CONCEPTS THEORIQUES ET PROBLEMATIQUE

---

L'objectif de ce chapitre est de présenter les notions théoriques relatives à notre sujet d'étude et préciser la raison d'être de notre travail. Nous commencerons par présenter le vocabulaire de l'archivage ensuite celui du Cloud et enfin celui de la cryptographie. La problématique fera l'objet de la seconde partie.

### Sommaire

<b>1.1</b>	<b>Vocabulaire de l'archivage</b>	<b>5</b>
1.1.1	Concept d'archives	5
1.1.2	Concept d'archivage	5
1.1.3	Acteurs	5
1.1.4	Document	6
1.1.5	Données	6
1.1.6	Support	6
1.1.7	Dossier	6
<b>1.2</b>	<b>Vocabulaire du Cloud</b>	<b>6</b>
1.2.1	Concept de Cloud	6
1.2.2	L'archivage cloud	7
<b>1.3</b>	<b>Vocabulaire de la cryptographie</b>	<b>7</b>
1.3.1	Chiffrement symétrique	7
1.3.2	Chiffrement asymétrique	8
<b>1.4</b>	<b>Problématique</b>	<b>8</b>

---

## 1.1 Vocabulaire de l'archivage

### 1.1.1 Concept d'archives

D'après l'article 2 de la loi N°2000/010 du 10 décembre 2000 régissant les archives au Cameroun , « les archives sont l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leurs activités ». Pour Bruno DELMAS (DELMAS (Bruno); Notions générales d'archivistique , en ligne<sup>1</sup> ) professeur d'archivistique, de diplomatique et d'institutions de l'époque contemporaine, à l'Ecole nationale des chartes en France, souligne que le mot "archives" peut désigner trois réalités très différentes :

- les documents qui font l'objet de la conservation ;
- les services ou bureaux dont la fonction est de gérer les documents d'archives ;
- les locaux et bâtiments dont la fonction est de conserver des documents et de loger les services qui en sont chargés.

### 1.1.2 Concept d'archivage

L'**archivage** est défini comme l'« Action de conserver et de classer des documents ne présentant plus un intérêt immédiat » (Pierre LAROUSSE ; Dictionnaire de français Larousse ; en ligne<sup>2</sup>) . En d'autres termes, c'est la démarche d'organisation qui a pour objectif d'identifier, de mettre en sécurité et de maintenir disponibles l'ensemble des documents qui engagent une entreprise ou un organisme vis-à-vis de tiers ou de son activité future et dont le défaut représenterait un risque.

### 1.1.3 Acteurs

« Les acteurs sont les personnes ou profils chargés d'une activité particulière dans le projet d'archivage. On distingue cinq profils : le management, la coordination (du projet puis du système d'archivage), l'expertise juridique ou métier des documents, la gestion technique du stockage et de la conservation, et les utilisateurs qui produisent ou utilisent les documents archivés ». ( CHABIN (Marie) ; Nouveau glossaire de l'archivage ; en ligne<sup>3</sup>)

---

1. ; <http://www.piaf-archives.org/se-former/module-2-notions-generales-archivistique>

2. <http://www.larousse.fr/dictionnaires/francais/archivage/5085?q=archivage#5060> ;

3. [docplayer.fr/345979-Nouveau-glossaire-de-l-archivage.html](http://docplayer.fr/345979-Nouveau-glossaire-de-l-archivage.html) ;

#### 1.1.4 Document

« Un document désigne un objet constitué d'un support et de l'information qu'il porte, considéré comme un tout signifiant».(**CHABIN(Anne Marie)** ; Nouveau glossaire de l'archivage ;en ligne <sup>4</sup> ;)

#### 1.1.5 Données

Une données peut être un « mot, nombre, signal, chaîne de caractères, séquence de bits, morceau de matière ou tout autre élément brut enregistré dans un système d'information où il pourra être corrélé à d'autres objets et interprété pour constituer une information».(**CHABIN(Anne Marie)** ; Nouveau glossaire de l'archivage ;en ligne <sup>5</sup> ;).

#### 1.1.6 Support

Un support est un «élément matériel sur lequel est enregistrée l'information pour produire un document et qui sert à la fois à le transmettre et à le conserver».(**CHABIN(Anne Marie)** ; Nouveau glossaire de l'archivage ;en ligne <sup>6</sup> ;).

#### 1.1.7 Dossier

Lorsqu'une personne ou une institution, dans le cours de ses activités, réunit plusieurs pièces pour traiter une affaire donnée, elle constitue ce que l'on appelle un dossier , le dossier de l'affaire qui est un ensemble organique de documents. En d'autres mots, le dossier désigne l'« ensemble organisé de documents liés entre eux par leur objet ou leur usage, constitué au cours d'une période donnée définie par les date d'ouverture et date de clôture du dossier. » (**CHABIN(Anne Marie)** ; Nouveau glossaire de l'archivage ;en ligne <sup>7</sup> ;).

### 1.2 Vocabulaire du Cloud

#### 1.2.1 Concept de Cloud

Pour **Alain TCHANA**, professeur à l'Institut National Polytechnique de Toulouse IRIT,« le **Cloud** (nuage en français) désigne l'ensemble de ressources, applications ou services s'exécutant dans un environnement distribué, accessible via les protocoles web standards, et dont l'ensemble fournit un service ayant les caractéristiques suivantes :

---

4. Op.cit

5. Op.cit

6. Op.cit

7. Op.cit



- Paiement à l'usage ;
- Fonction de la durée et de la quantité d'utilisation ;
- Illusion d'une infinité de ressources ;
- Abstraction de l'infrastructure matérielle ;
- Mutualisation entre plusieurs utilisateurs.

»(TCHANA(Alain) ; Le Cloud : généralités ; Support de cours 2017 ; Page 16)

### 1.2.2 L'archivage cloud

A partir des définitions précédentes, on peut considérer l'**archivage cloud** comme l'externalisation de documents et de données sur des serveurs distants grâce à Internet.

## 1.3 Vocabulaire de la cryptographie

Le mot **cryptographie** provient de deux vocables grecs :

- *Kruptos* qui signifie *caché*
- et *Graphein* qui signifie *écrire*

La **cryptographie** est donc l'une des disciplines de la cryptologie<sup>8</sup> s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de clés. Un système cryptographique est un ensemble composé de

- un algorithme de chiffrement ***E***
- un algorithme de déchiffrement ***D***
- tous les textes clairs possibles ***M***
- tous les textes chiffrés ***C***
- toutes les clés. ***K*** Lorsque la clé de chiffrement est aussi celle de déchiffrement on parle de *Chiffrement symétrique*.

### 1.3.1 Chiffrement symétrique

Pour cette technique, l'émetteur et le destinataire du message disposent de la même clé secrète ***k***. L'émetteur va utiliser cette clé secrète ***k*** pour chiffrer le message ***M***. Le message chiffré est ***C***. Le récepteur utilisera cette même clé secrète ***k*** pour déchiffrer le message chiffré ***C***, et retrouver ainsi le message en clair ***M*** d'origine. Cette technique est illustrée dans la figure 1.1 ci-dessous.

---

8. *Cryptologie* signifie littéralement science du secret et a pour objet de cacher les informations d'un message

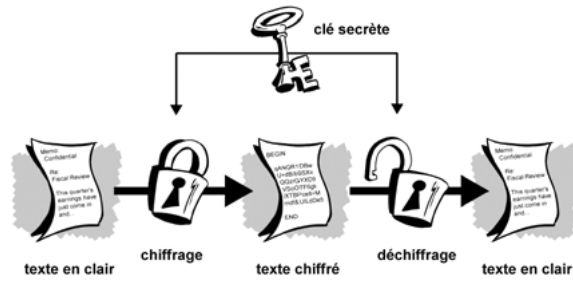


FIGURE 1.1 – Principe du chiffrement symétrique  
9

### 1.3.2 Chiffrement asymétrique

Cette technique repose sur le fait que la clé de chiffrement soit différente de la clé de déchiffrement. De plus, la clé de déchiffrement ne peut pas être calculée à partir de la clé de chiffrement et réciproquement. La clé de chiffrement appelée clé publique est destinée à être divulguée, tandis que la clé de déchiffrement appelée clé privée est gardée secrète. Dans ce cas, la procédure à suivre est la suivante :

- l'émetteur doit récupérer la clé publique **k1** du destinataire avec laquelle il va chiffrer le message en clair **M**. Puis il va envoyer le message chiffré résultant **C** au destinataire ;
- ainsi le destinataire peut déchiffrer ce message chiffré **C** avec sa clé privée **k2** et retrouver le message en clair **M** d'origine. Cette technique est illustrée dans la figure 1.2 ci-dessous.

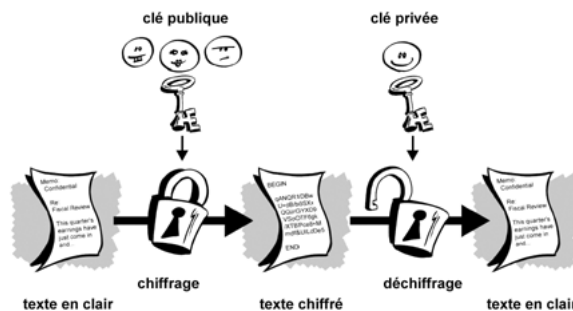


FIGURE 1.2 – Principe du chiffrement asymétrique  
10

## 1.4 Problématique

En matière de gestion documentaire, les entreprises évoluent dans un environnement toujours plus complexe et évoluant toujours plus vite. Elles doivent faire face à un volume de documents croissant de manière exponentielle, qu'elles doivent archiver physiquement, électroniquement, voire les deux, le tout dans un contexte légal strict et sous des contraintes de rentabilité fortes. Les facteurs tels que les moyens financiers et la sensibilité des données

expliquent le choix des entreprises actuelles à conserver soi-mêmes leurs archives, d'autres à sous-traiter ceux-ci. Au regard du volume des archives, de leur l'importance croissante pour toute entreprise, ainsi que la sécurité de l'entreprise elle-même, on ne peut s'empêcher de se poser les questions suivantes :

- Pouvons-nous réellement sous-traiter l'archivage électronique des informations très souvent sensibles, en texte clair et parler de sécurité de l'entreprise ?
- Comment garantir simultanément la disponibilité des archives électroniques et la confidentialité de celles-ci ? Telles sont les questions constitutives de la problématique, auxquelles il sera question d'apporter une réponse dans la suite de ce travail.

*Ce chapitre nous a permis d'appréhender le monde de l'archivage numérique, de nous familiariser au Cloud Computing, de décrire les principes de base de la cryptographie et de préciser la raison d'être de notre travail.*

# 2

## ETAT DE L'ART

---

Dans ce chapitre, il est question premièrement de présenter les déclinaisons des offres d'archivage numérique dans le cloud, et deuxièmement, exposer notre contribution. Une offre de service cloud a vocation à bénéficier d'une économie d'échelle, et donc à mutualiser tout ou partie des couches . Pour cette raison, elle est nécessairement plurielle, de sorte que l'on pourrait distinguer plusieurs types d'approches d'archivage cloud, plusieurs catégories d'archivage en la matière.

### Sommaire

---

<b>2.1</b>	<b>Types d'approches d'archivage cloud</b>	<b>11</b>
2.1.1	Archivage sur le Cloud : approche Cloud public	11
2.1.2	Archivage sur le Cloud : approche Cloud privé	11
2.1.3	Le Cloud hybride	11
2.1.4	Le Cloud communautaire	12
<b>2.2</b>	<b>Présentation des catégories existantes d'archivage selon les approches de services Cloud</b>	<b>12</b>
2.2.1	L'approche IaaS de l'archivage sur le cloud : externalisation partielle de l'infrastructure matérielle	12
2.2.2	L'approche Software as a Service (SaaS) de l'archivage sur le cloud : internalisation totale de l'infrastructure matérielle	13
2.2.3	L'approche Platform as a Service (PaaS) de l'archivage sur le cloud : externalisation totale de l'infrastructure matérielle, des environnements et des données	15
2.2.4	Modes d'archivage hybrides	15
2.2.5	Archivage sur le cloud : Synthèse	16
<b>2.3</b>	<b>Insuffisances sécuritaires des catégories existantes d'archivage selon les approches de services Cloud</b>	<b>16</b>

---

## **2.1 Types d'approches d'archivage cloud**

Selon la multiplicité des répartitions d'accès aux services cloud, on distingue généralement 4 types d'approches : l'approche Cloud public, l'approche Cloud privé, l'approche Cloud hybride et l'approche Cloud communautaire.

### **2.1.1 Archivage sur le Cloud : approche Cloud public**

On parle de Cloud public lorsque les services de Cloud sont potentiellement disponibles pour n'importe quel client, personne publique ou personne privée. Les frontières d'un Cloud public sont imprécises, et le client n'a quasiment aucune restriction pour accéder à l'ensemble des services de ce type de Cloud, que les données le concernent ou pas. AWS, Microsoft, Google et Rackspace sont quelques actuels fournisseurs de Cloud public leaders du marché. Pour ce qui concerne l'archivage dans le Cloud, il est en fait une possibilité d'archivage dans un ou plusieurs « Clouds » publics. Pour simplifier prenons l'exemple d'un seul. Du côté du fournisseur la mutualisation peut concerner tout ou partie des couches, depuis l'infrastructure de calcul et de stockage jusqu'au logiciel d'archivage. La question se pose en particulier de la mutualisation des archives des différents clients. Or la crédibilité s'établit dans la durée, et se perd très vite en cas de problème. Du côté du client <sup>1</sup>, la mutualisation des données est généralement perçue comme un risque. La vérification du niveau de service rendu est plus difficile, et il faudrait un avantage prix important pour que cette perception de risque soit acceptable.

### **2.1.2 Archivage sur le Cloud : approche Cloud privé**

Le Cloud privé est modèle de déploiement dans lequel les services de cloud sont utilisés exclusivement par un seul client, qui en contrôle les ressources. Un cloud privé peut être mis en œuvre soit par l'organisation à laquelle appartient le client soit par un prestataire externe. Un cloud privé a vocation à borner précisément ses limites et à restreindre l'accès à ses services à une organisation unique. DropBox, Microsoft OneDrive, Google Drive, Mega sont quelques fournisseurs de Cloud privé.

### **2.1.3 Le Cloud hybride**

Le Cloud hybride est modèle de déploiement mélangeant à la fois des offres de cloud privé et de cloud public en fonction des besoins et des typologies de données, destiné notamment à répondre aux pics de charge. Il y a plusieurs manières de déployer du Cloud Hybride, par exemple :

---

1. Client en tant que personne morale

- en s'appuyant sur différents fournisseurs de Cloud.
- en s'appuyant sur un fournisseur unique qui propose ces 2 modèles.
- en possédant son propre Cloud privé et en souscrivant à un fournisseur de Cloud hybride, par exemple : HP, IBM, Microsoft, Oracle.

#### **2.1.4 Le Cloud communautaire**

Le cloud communautaire se rapproche du Cloud public mais, est exclusivement réservé à des clients dont les caractéristiques et les besoins sont similaires, souvent dans le cadre d'un groupement. Comme exemple de Cloud communautaire, citons :

- La GSA (General Services Administration) aux Etats Unis, qui a lancé un site communautaire pour les organisations gouvernementales américaines.
- Amadeus, principal fournisseur de solutions informatiques à l'industrie du tourisme et du voyage, crée par Air France, Lufthansa, Iberia et SAS il y a 20 ans. C'est aujourd'hui le premier acteur mondial dans le domaine des voyages, avec plus de 150 compagnies aériennes clientes, 280 millions de transactions quotidiennes et 2 500 informaticiens mobilisés. Son principe est celui de proposer des applications métiers en mode SaaS à toutes ses entreprises clients via un seul et unique logiciel. On ajoutera à ces notions celle de Cloud souverain, c'est-à-dire un Cloud dont les données sont entièrement stockées et traitées sur le même territoire et dont le client connaît précisément la localisation.

## **2.2 Présentation des catégories existantes d'archivage selon les approches de services Cloud**

Une offre d'archivage cloud peut proposer plusieurs catégories de services :

### **2.2.1 L'approche IaaS de l'archivage sur le cloud : externalisation partielle de l'infrastructure matérielle**

L'infrastructure en tant que service IaaS est un modèle de Cloud Computing dans lequel :

- Un prestataire fournit l'infrastructure et la solution d'archivage :
  - le ou les serveurs ;
  - les couches de virtualisation ;
  - 2. le stockage ;
  - 3. les réseaux.
- L'entreprise utilisatrice gère :
  - 1. le système d'exploitation des serveurs ;
  - 2. les logiciels applicatifs dont celui du SAE.

## **SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD**

L'entreprise utilisatrice fait donc l'acquisition des licences pour le SAE et prend à sa charge la mise en œuvre de ce logiciel. Elle loue auprès du prestataire une infrastructure Cloud comprenant des serveurs, du stockage et du réseau avec un modèle de paiement en fonction de l'utilisation. Elle accède à cette infrastructure sur Internet pour mettre en œuvre et gérer son SAE. Trois caractéristiques majeures ressortent de cette approche.

#### **2.2.1.1 Gestion des ressources IaaS par l'entreprise utilisatrice**

Les offres IaaS reposent sur des techniques de virtualisation. L'entreprise utilisatrice construit son infrastructure d'archivage électronique et la fait évoluer selon ses besoins : ressources Central Processing Unit (CPU), mémoire, espaces de stockage, bande passante réseau, firewall dédié, gestion des comptes utilisateurs.

#### **2.2.1.2 Mise en place d'un réseau sécurisé**

Dans la majorité des cas, pour accéder aux serveurs en mode IaaS, un Virtual Private Network (VPN) permet de relier l'entreprise utilisatrice avec le prestataire. La garantie de qualité de service et de sécurité des réseaux est du ressort de prestataires de télécommunications.

#### **2.2.1.3 Délégation de la sécurité IaaS auprès du prestataire**

Le prestataire IaaS prend en charge l'hébergement et la sécurité physique du matériel lié aux supports d'archivage et aux serveurs : redondance des équipements, sécurité 24/24 et 7/7, surveillance vidéo, climatisation, détection incendie. La sécurité applicative est assurée par des services d'authentification mis en place par le prestataire. L'exploitation est réalisée par le prestataire.

### **2.2.2 L'approche Software as a Service (SaaS) de l'archivage sur le cloud : internalisation totale de l'infrastructure matérielle**

La solution logicielle en tant que service SaaS est un modèle de Cloud Computing dans lequel :

- Un prestataire fournit à la fois l'infrastructure et la solution d'archivage :
  - le ou les serveurs ;
  - les couches de virtualisation ;
  - le stockage ;
  - les réseaux ;
  - le système d'exploitation des serveurs ;
  - les logiciels applicatifs dont celui du SAE.

- L'entreprise utilisatrice loue auprès du prestataire un service tarifié notamment selon :
  - des licences pour le SAE sur la base d'un loyer mensuel incluant la maintenance logicielle ;
  - une infrastructure cloud nécessaire (serveurs, stockage et réseau avec un modèle de paiement en fonction de l'utilisation) ;
  - les autres types de services spécifiés contractuellement.

L'entreprise utilisatrice consomme alors la solution d'Archivage Electronique à la demande, en fonction de ses besoins réels. Relevons quelques caractéristiques majeures :

#### **2.2.2.1 Gestion des ressources IaaS par l'entreprise utilisatrice**

Les offres SaaS reposent aussi sur des techniques de virtualisation. Le prestataire gère l'infrastructure d'archivage électronique et la fait évoluer selon les besoins de l'entreprise utilisatrice : ressources CPU, mémoire, espaces de stockage, bande passante réseau, firewall dédié, gestion des comptes utilisateurs.

#### **2.2.2.2 Délégation de la sécurité SaaS auprès du prestataire**

En plus des garanties offertes par le fournisseur IaaS, le prestataire SaaS prend en charge la sécurité du système d'archivage électronique. La sécurité applicative est assurée par des services d'authentification mis en place par le prestataire. L'exploitation de la solution est réalisée par le prestataire.

#### **2.2.2.3 Mise en place d'une communication sécurisée**

Pour accéder à sa solution d'Archivage Electronique en mode SaaS, une communication sécurisée entre le client et son prestataire est mise en place. Des protocoles de communication sécurisés (ftps, https, ...) sont mis en œuvre pour les différentes fonctions du SAE (versement, communication, ...). L'entreprise utilisatrice loue auprès du prestataire un service tarifié notamment selon :

- Des licences pour le SAE sur la base d'un loyer mensuel incluant la maintenance logicielle ;
- Une infrastructure cloud nécessaire (serveurs, stockage et réseau avec un modèle de paiement en fonction de l'utilisation) ;
- Les autres types de services spécifiés contractuellement.

## **SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD**



### **2.2.3 L'approche Platform as a Service (PaaS) de l'archivage sur le cloud : externalisation totale de l'infrastructure matérielle, des environnements et des données**

Platform as a Service, souvent appelé simplement PaaS, est une catégorie de services de Cloud Computing qui fournit la plateforme et l'environnement informatique nécessaire aux développeurs (généralement) pour mettre en place leurs différents services et applications sur Internet. Les services PaaS sont hébergés dans le Cloud et les utilisateurs y accèdent simplement, par leur navigateur web.

### **2.2.4 Modes d'archivage hybrides**

Traditionnellement, les systèmes d'archivage sont mis en œuvre en interne. Sur la base des différents services possibles (SaaS, PaaS, IaaS), plusieurs architectures peuvent se décliner, mixant approche interne et cloud jusqu'à une externalisation complète. Un système d'archivage hybride peut, de façon très synthétique, être découpé en trois sous-ensembles :

- Les fonctions de stockage ;
- Des fonctions contribuant à la valeur probatoire ;
- La politique d'archivage et les fonctions de référencement. C'est dans la répartition de ces ensembles que les solutions intermédiaires pourront varier. Les motivations des entreprises sont principalement de l'ordre de l'optimisation financière tout en conservant en interne la maîtrise de certains composants jugés critiques ou à risques.

#### **2.2.4.1 Les fonctions de stockage**

Dans les systèmes d'archivage, les fichiers sont en général stockés au moins en deux exemplaires afin d'offrir des garanties de pérennité. Le stockage des fichiers dans le Cloud peut porter sur l'ensemble de ces instances ou seulement une partie d'entre elles (IaaS et SaaS), les autres restants alors stockées en interne. Dans ce type de configuration, il sera nécessaire d'être extrêmement vigilant sur les acquittements touchant aux opérations sur les fichiers .

#### **2.2.4.2 Les fonctions contribuant à la vocation probatoire**

Les fonctions contribuant à la vocation probatoire peuvent être portées :

- par le logiciel d'archivage (SaaS ou PaaS) ;
- par l'infrastructure de stockage sécurisée(IaaS) ;
- par une combinaison logiciel/infrastructure (SaaS, IaaS, PaaS).

Au-delà de ces répartitions des ensembles fonctionnels, il faut également considérer que la configuration du système d'archivage peut être modulée en fonction des types de documents

## **SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD**

ainsi que des contraintes et risques qui y sont associés dans la mesure où les systèmes d'archivage peuvent piloter la stratégie de stockage en fonction des règles. Ainsi une solution d'archivage hébergée en interne et disposant également d'espaces de stockage internes et externes dans le Cloud peut, par exemple, s'orienter :

- Vers les espaces de stockage internes pour certains types de données comme les données à caractères personnels ou les documents confidentiels ;
- A la fois vers les espaces internes et les espaces externes (une instance de chaque côté) pour les types de données nécessitant une consultation ou une remise en ligne rapide ;
- Vers les espaces de stockage externes pour les autres types de données.

#### **2.2.4.3 3 La politique d'archivage et les fonctions de référencement**

Les fonctions de référencement sont l'aboutissement formel de la politique d'archivage mise en œuvre dans l'entreprise. Elles facilitent les recherches. Cette politique décrit entre autres les charges de stockage de fichier entre le prestataire et le client ainsi que les durées de stockage. D'où son caractère hybride.

#### **2.2.5 Archivage sur le cloud : Synthèse**

En fonction de la catégorie de service cloud et des charges de l'entreprise dans le processus d'archivage, on distingue 4 formes de SAE. Elles sont clairement décrites dans la figure 2.1 ci-dessous :

- **IaaS** infrastructure à la charge du fournisseur
- **PaaS** infrastructure et prérequis à la charge du fournisseur
- **SaaS** service d'archivage à la charge du fournisseur

### **2.3 Insuffisances sécuritaires des catégories existantes d'archivage selon les approches de services Cloud**

La préoccupation la plus évidente lorsque l'on souhaite bâtir une archive en nuage est celle de la sécurité. Cette préoccupation peut s'exprimer de la manière suivante : Comment la protection des données sera-t-elle assurée à la fois durant le transit à travers le réseau et au repos une fois que ces données sont dans le centre de données du fournisseur de service ? L'offre existante de l'archivage Cloud répond à sa manière à cette préoccupation. Par rapport au transit, la réponse est satisfaisante à notre sens. Le transfert se faisant en général via des protocoles web au-dessus d'un lien sécurisé via HTTPS (chiffrement SSL), les données transférées à travers le réseau public seront en sécurité en vol. Par ailleurs, la plupart des fournisseurs offrent désormais la possibilité de chiffrer les données stockées dans leurs nuages.

#### **SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD**

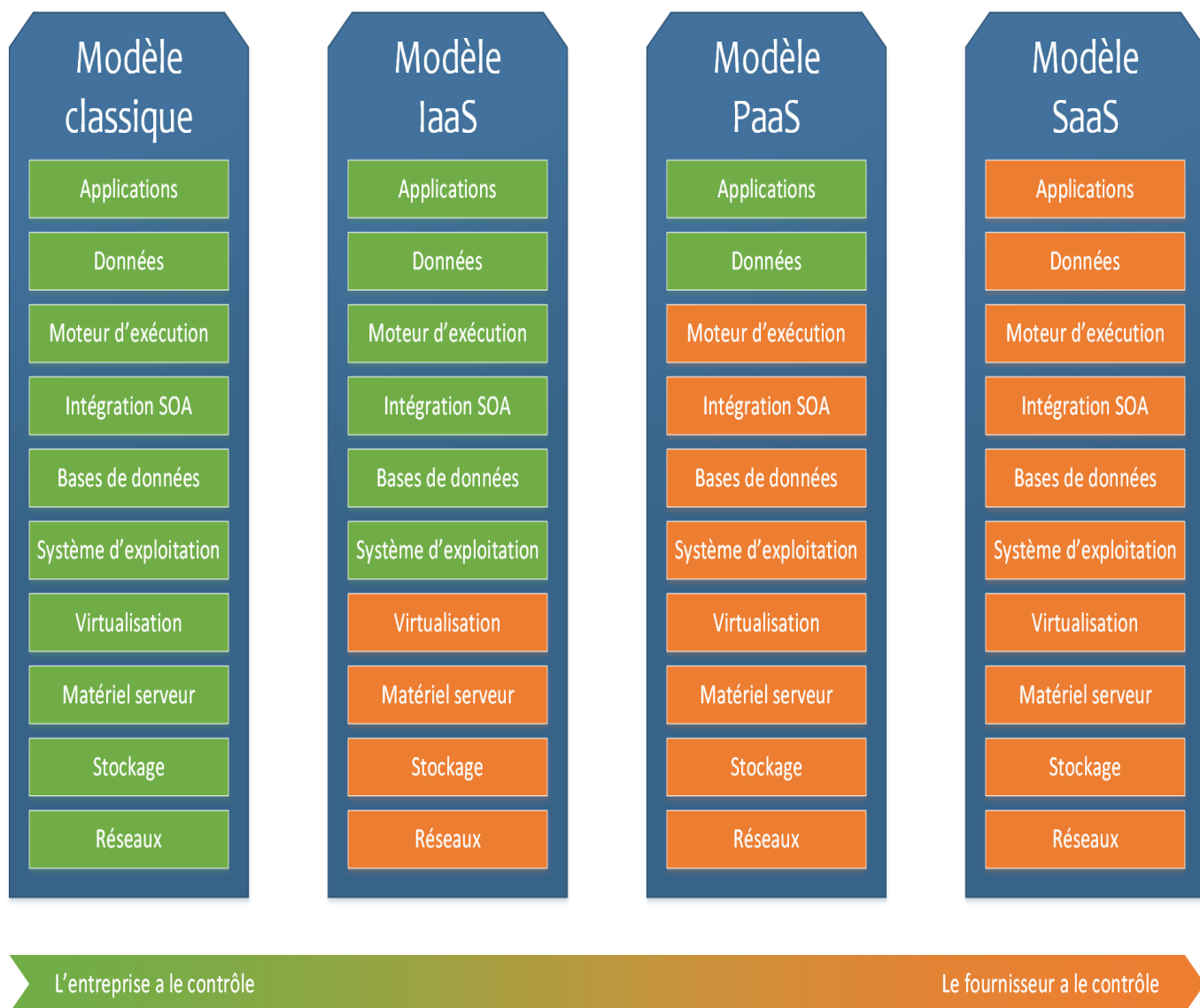


FIGURE 2.1 – Description de différentes formes de SAE en fonctions de la répartition des services entre l'entreprise et le fournisseur de service Cloud

Afin de disposer d'un niveau de sécurité supplémentaire, les clients peuvent fournir leurs propres clés de chiffrement à utiliser par le fournisseur pour chiffrer les données pour le compte du client. Et c'est à ce stade de repos que la sécurité nous apparaît comme mise en mal.

Confier en effet la sécurité des informations, surtout celle des plus intimes, à un prestataire sans les chiffrer d'avance peut à la longue se révéler fatal. Le même prestataire peut à l'insu du client déchiffrer ces informations et même les diffuser. C'est là que se trouve la faiblesse du système !

Le chapitre suivant aura donc à cet effet d'exposer la méthodologie qui va servir à la construction de la tentative de solution à cette difficulté.

## SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD

# 3

## METHODOLOGIE

---

Afin de fournir une description de la solution SCAE-CPC à notre problématique, il convient de préalablement décrire la politique de sécurité, ensuite exposer les besoins exprimés par les utilisateurs.

### 3.1 Description de SCAE-CPC

Disposer des informations adéquates à long terme implique l'archivage des données, mais aussi des fichiers, tables et paramètres. Cet archivage doit présenter des garanties suffisantes en termes de conservation et de préservation de l'intégrité. Au lieu de soumettre simplement les données au service du prestataire, nous préconisons l'option consistant à chiffrer préalablement celles-ci avant de les soumettre. C'est donc une nuance de l'approche IaaS que nous avons développée au Centre Pasteur du Cameroun (CPC) suivant une méthodologie consistant à décrire le périmètre d'archivage, la volumétrie des données, la nature de l'archivage, le support de conservation, la consultation, les formes de restitution, la gestion des autorisations, le classement et l'identification des archives, et enfin la politique de destruction adoptée. Notre contribution est schématiquement illustrée sur la figure 3.1 ci-dessus. Voici d'avantages de précisions sur les mesures prises afin d'élever le niveau de sécurité des archives.

#### 3.1.1 Le périmètre d'archivage

Une politique d'archivage est nécessairement délimitée par un périmètre d'application. Ce cadre doit légitimer la progression de la démarche d'archivage<sup>1</sup>. Ce périmètre est triple et s'applique :

---

1. Records management

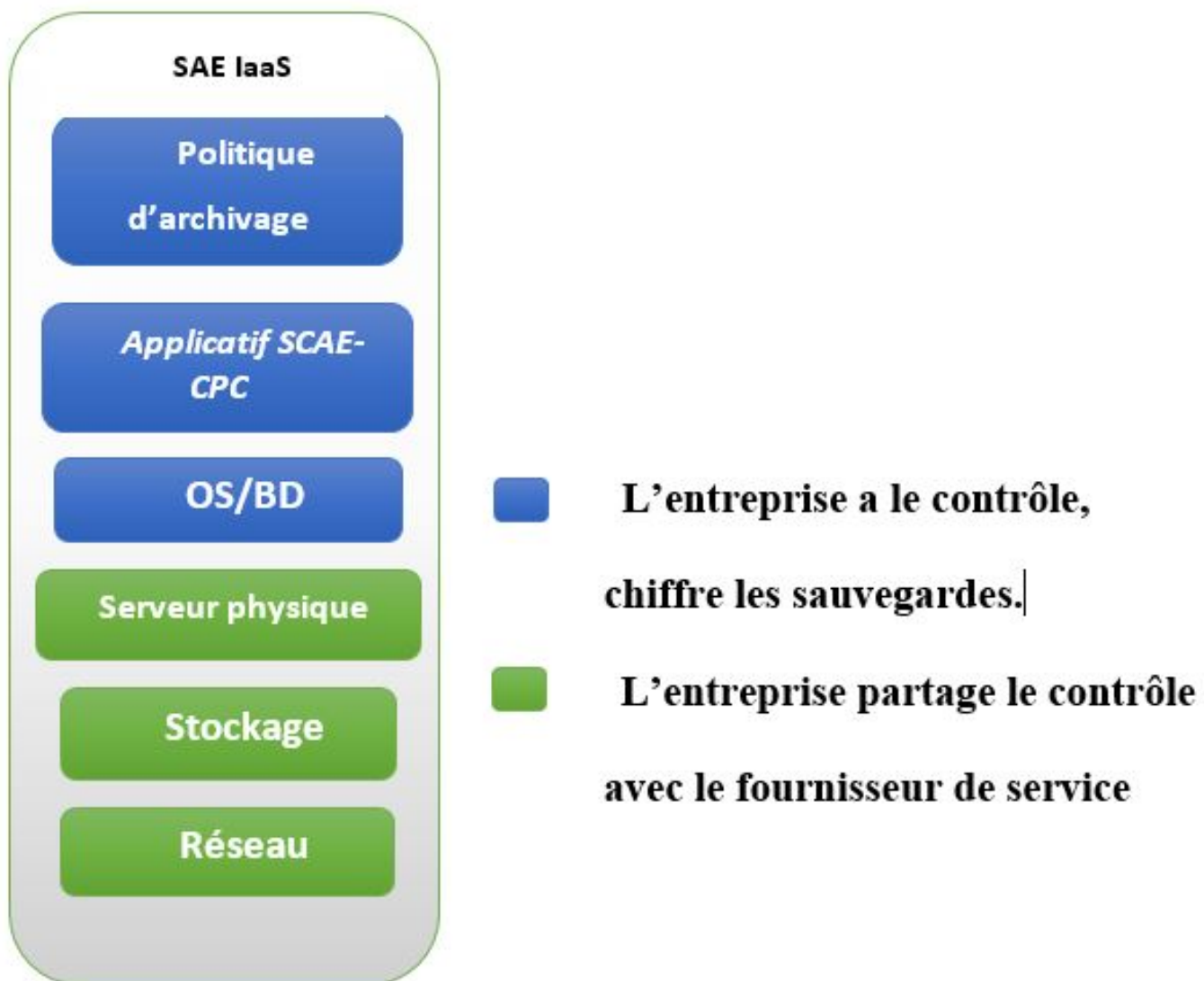


FIGURE 3.1 – Illustration de la forme de SAE mise en œuvre dans SCAE-CPC

#### 3.1.1.1 Aux documents à archiver

La lecture de l'article 2 alinéa 3 primo de la loi N°2000/010 du 10 décembre 2000 régissant les archives au Cameroun<sup>2</sup> permet de catégoriser les archives au Cameroun. Le CPC étant un établissement parapublic, l'ensemble des documents qu'il est appelé à produire sont classés "archives publiques". Spécifiquement, au CPC l'archivage sur support informatique doit porter sur : les livres comptables légaux , le fichier des écritures comptables, les pièces

2. « Les archives publiques sont constituées par :

— les documents qui procèdent de l'activité de l'Etat, des collectivités territoriales décentralisées, des établissements publics et des entreprises du secteur public et parapublic ;... »

justificatives dématérialisées, le plan comptable de l'entreprise, la table des taux de TVA, le fichier d'inventaire, les données de gestion des immobilisations (validation des montants de dotations aux amortissements...), la comptabilité analytique ou budgétaire, les éléments de calcul des dépréciations et provisions, la détermination de coûts de production, d'achat, de revient ou de transfert, des marges, les factures d'achats les factures de ventes, des résultats des différents laboratoires...

#### **3.1.1.2 À toutes les composantes de l'entreprise**

Dans le cadre de notre travail, tous les départements pourront bénéficier des services du SCAE-CPC.

#### **3.1.1.3 Aux personnes en interaction avec l'entreprise (collaborateurs – prestataires)**

### **3.1.2 La volumétrie des données à archiver**

En tant que laboratoire de prélèvements et d'analyses médicales doté d'une forte administration, le CPC utilise l'outil informatique comme support de collecte des prélèvements, de traitement des données, de communication interne<sup>3</sup> et externe<sup>4</sup>. Toutes ces informations doivent être efficacement sauvegardées. Le volume des données à archiver par le SCAE-CPC est de l'ordre du Téra Octet.

#### **3.1.3 Nature de l'archivage**

La lecture de l'article 8 de la loi N°2000/010 du 10 décembre 2000 régissant les archives au Cameroun<sup>5</sup> laisse croire que les archives du CPC sont des archives courantes. A côté des archives courantes l'on peut néanmoins recenser les autres formes d'archives à savoir, les archives intermédiaires et les archives historiques. Indépendamment de cette classification par nature, l'article 11 alinéa 1 de la loi précitée dispose que les archives ne peuvent être éliminés avant un délai de 10 ans à compter de la date de sa production ou de sa réception .

---

3. Entre le personnel

4. Retrait des résultats d'examen et des annonces

5. « Les archives courantes sont constituées par les documents d'utilisation fréquente, pour l'activité des administrations, des services, établissements ou organismes qui les ont produits ou reçus » Cet article dispose in extension que : « Aucun document d'archives publiques ne peut être éliminé avant un délai de dix(10) ans à compter de la date de sa production ou de sa réception. »

### 3.1.4 La valeur probante de l'archivage numérique

Alors que la question de la valeur probatoire de l'archivage numérique n'est pas encore résolue en droit camerounais, le droit positif français à titre de droit comparée fournit une réponse à cette question : « l'écrit sur support électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité » . Par conséquent, il faut, selon le droit français, remplir deux conditions pour que l'écrit numérique soit admis comme une preuve :

- il faut pouvoir connaître son origine (il s'agit donc de savoir quelle est la personne physique ou morale qui porte la responsabilité du document numérique) ;
- l'écrit numérique doit être établi et conservé dans des conditions de nature à conserver son intégrité.

Ce régime juridique français de la valeur probatoire de l'archivage numérique peut très bien être transposé dans le droit positif camerounais. Il suffira alors de considérer les dispositions de l'article 256-1<sup>6</sup> et 256-2<sup>7</sup> de l'Acte uniforme relatif au droit des sociétés commerciales et du groupement d'intérêt économique (AUSCGIE) qui consacre la possibilité d'opérer les formalités de constitution de la société commerciale par voie électronique. L'on s'imagine alors que le mécanisme de preuve de telles formalités peut également servir en matière d'archivage numérique.

Dans cette logique, pour remplir les deux conditions sus évoquées lors d'une transaction en ligne dans le cadre de SCAE-CPC, on devrait avoir recours à la technique de la signature électronique. La signature électronique permet, par un procédé cryptographique, de garantir l'intégrité du document signé et l'identité du signataire. La cryptographie est une technique ayant pour but de chiffrer un message, c'est-à-dire de le rendre inintelligible aux yeux de ceux qui ne sont pas les destinataires du message. Les clés sont choisies de façon transparente aux utilisateurs, c'est-à-dire à l'insu des utilisateurs. Ainsi, seuls ceux disposants des droits pourront accéder au contenu des fichiers.

### 3.1.5 Consultation et restitution des archives

Il s'agira ici de répondre à la question de savoir : Comment permettre la consultation et la restitution des archives dans des délais compatibles avec les contraintes légales et/ou requis par les utilisateurs potentiels ? Dans le cadre du SCAE-CPC, nous avons mis en œuvre une astuce consistant à constituer premièrement les sauvegardes

---

6. « Les formalités relatives aux sociétés peuvent être effectuées par voie électronique conformément aux dispositions du livre V de l'Acte uniforme sur le droit commercial général ainsi qu'aux dispositions applicables du présent Acte uniforme »

7. « Les formalités de publicité par dépôt d'actes ou de pièces prévues par le présent Acte uniforme sont effectuées au greffe de la juridiction ou de l'organe compétent dans l'Etat Partie du lieu du siège social. ... Le Bulletin national peut être publié sur support papier ou sous forme électronique. ... »

cryptées qui seront stockées dans le serveur local. Ce qui facilitera la consultation par les utilisateurs locaux. Ces sauvegardes constituées par le service des archives qui seront archivées dans le cloud selon les contrats avec le prestataire cloud.

### 3.1.6 Forme de restitution des données

Les données seront restituées numériquement dans le cadre du SCAE-CPC

### 3.1.7 Gestion des autorisations d'accès

La multiplicité des documents à traiter et les habituelles procédures mises en place lors de l'archivage manuel rendent la question complexe. Dans le cadre du SCAE-CPC, quelques principes dirigent l'accès aux documents :

- tous les documents conçus dans un département sont accessibles au personnel de ce département ;
- les documents conçus dans un département ne sont accessibles au personnel d'un autre département qu'après autorisation du chef du département source du document ;
- néanmoins les documents personnels tels que les contrats d'emplois, les bulletins de payes sont accessibles au possesseur de document sans contrainte.

### 3.1.8 Classement et identification des archives

Cette section est une réponse à la question de savoir : comment classer les archives de manière à pouvoir les identifier ultérieurement ? La réponse à cette question sera traduite par trois principales activités :

- **Nommer les dossiers** : un intitulé, la typologie, les dates d'ouverture et de clôture de dossier permettront de retrouver facilement le document, d'appliquer les durées de conservation réglementaires et à terme, de trier efficacement les documents.
- **Organiser les dossiers** : cela relève de la responsabilité du département des archives, et pour leur faciliter le travail, le SCAE-CPC dispose d'une IHM facilitant la classification arborescente des sauvegardes.
- **Conserver les dossiers** : service d'archivage à la charge du fournisseur

Le cycle de vie d'un document d'archive se compose de trois phases : courante, intermédiaire et définitive. A chacune d'entre elles correspond un lieu de conservation spécifique. D'après la figure 3.2 ci-dessus, nous conservons les archives courantes en locale, les archives intermédiaires dans le Cloud et selon le règlement intérieurs, les archives définitives sont soit éliminées, soit définitivement conservées dans le Cloud.

## SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD



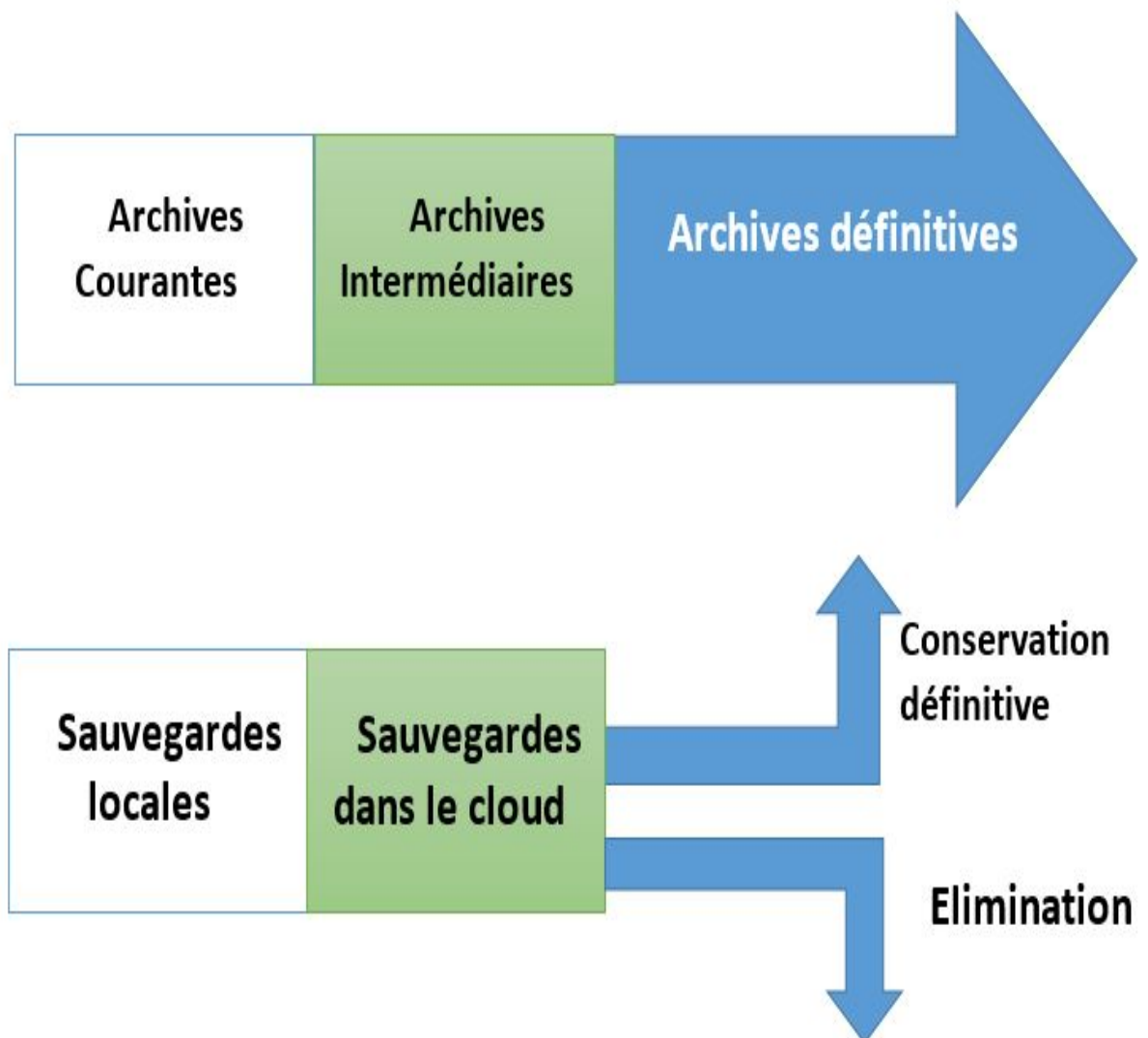


FIGURE 3.2 – Principe de conservation des documents dans SAE-CPC

### 3.1.9 Politique de destruction adoptée

D'après l'article 11 alinéas 3 de la loi N°2000/010 du 10 décembre 2000 régissant les archives au Cameroun, « la liste des documents destinés à l'élimination ainsi que les conditions de leur élimination, sont fixés en accord entre l'administration qui les a produits ou reçus et l'administration chargée des archives. ». Au CPC, les archives ne peuvent être détruites que 5 ans après leur création. De même, le SCAE-CPC n'autorisera pas la destruction d'une archive si ce n'est 5 ans après sa création.

## 3.2 Expression des besoins analyse et conception

L'expression des besoins décrit l'objet à développer en termes de fonctionnalités. En ce sens, elle répond à la question "quoi?". Durant cette phase, on effectue simultanément l'étude des données et l'étude des traitements à effectuer.

### 3.2.1 Les cas d'utilisation

Les cas d'utilisation constituent un moyen de recueillir et de décrire les besoins des acteurs du système. Nous présentons dans cette section l'ensemble des charges fonctionnelles et non fonctionnelles du SAE à mettre en place. Les acteurs du SAE sont classés en 4 catégories selon leur niveau d'accès aux données du CPC :

- ☞ Le personnel ;
- ☞ Le chef service ;
- ☞ L'archiviste ;
- ☞ L'administrateur.

Tout membre du personnel pourra effectuer les tâches suivantes dans le SCAE-CPC :

- ☞ s'inscrire ;
- ☞ s'authentifier ;
- ☞ sauvegarder un document (image, fichier) ;
- ☞ rechercher une archive ;
- ☞ pré-visualiser un document sauvegardé ;
- ☞ télécharger un document sauvegardé ;
- ☞ demander à consulter le document sauvegardé par un autre service. Le chef service, en plus des fonctionnalités accessibles au personnel
- ☞ autorisera ou refusera la consultation des documents de son service par un personnel d'un autre service. L'archiviste pourra
- ☞ éditer les métadonnées (service d'origine, auteur, objet, date de versement dans le système des archives, index, code, historique) ;
- ☞ décrire une archive ;
- ☞ modifier l'arborescence des sauvegardes ;
- ☞ rechercher une archive ;
- ☞ télécharger une archive ;
- ☞ pré-visualiser une archive ;
- ☞ gérer les droits d'accès des utilisateurs aux fichiers. Il reviendra à l'administrateur informatique de :

☞ choisir le prestataire de service cloud ;

☞ planifier l'archivage des données par ce prestataire de service cloud.

Le diagramme de la figure 3.3 ci-dessous est celui des cas d'utilisation. Ce diagramme représente les besoins des utilisateurs par rapport au système. Il constitue un des diagrammes de comportement les plus structurants dans l'analyse d'un système. (GABAY(Joseph), GABAY(David) ; UML2 Analyse et Conception ; DUNOD ; 2008 ; page 11)

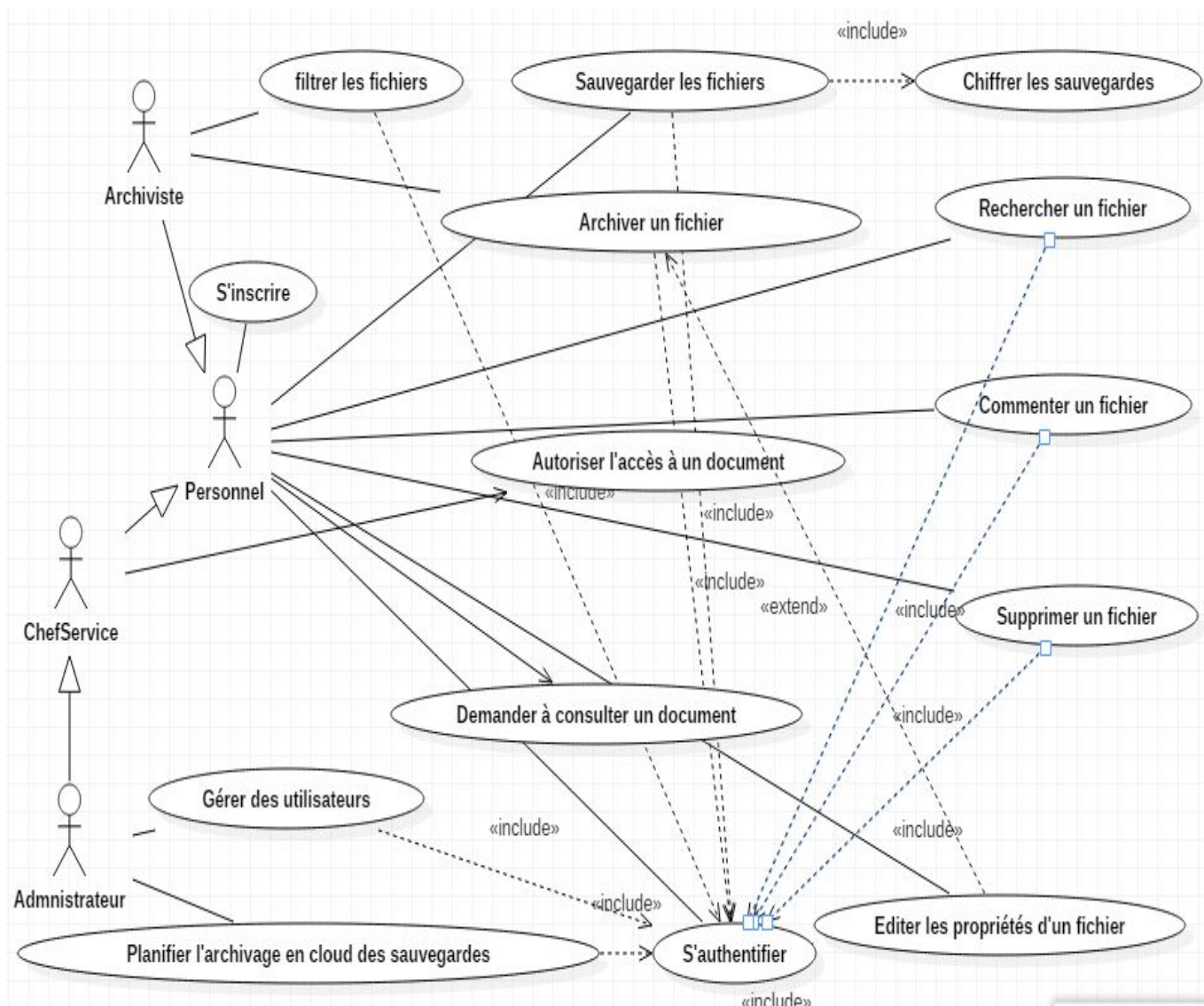


FIGURE 3.3 – Diagramme de cas d'utilisation

#### 3.2.1.1 Exigences de qualité

Eu égard aux habitudes d'archivage manuel de documents pratiquées ordinairement par le personnel Lambda, il nous importe d'attirer le personnel et le convaincre d'adopter notre nouvelle solution d'archivage électronique. Pour ce faire, il est important de répondre aux exigences de qualité suivantes :

- ☞ **Ergonomie sobre et efficace** Archiver les documents sur notre SAE ne doit pas prendre beaucoup de temps ou demander une grande connaissance scientifique. La mise en page du système facilitera au maximum la démarche à l'aide d'une présentation claire et intuitive.
- ☞ **La collecte facile des informations sur les archives** Les utilisateurs du SAE seront fréquemment appelés à renseigner beaucoup d'informations sur les documents à sauvegarder. A cause de la délicatesse, l'importance et la récurrence de cette tâche, nous automatiserons au mieux la collecte de ces informations de peur de rebuter les utilisateurs.

#### 3.2.1.2 Exigence de performance

Nous ne saurons négliger les exigences quantitatives suivantes, également très importantes pour les utilisateurs :

- ☞ Le SCAE-CPC doit pouvoir gérer autant de comptes utilisateurs que l'effectif du personnel de l'entreprise qui opte pour notre solution ;
- ☞ La multiplicité, la variété des média doit pouvoir être correctement gérées.

#### 3.2.1.3 Formulaire simple

Afin de ne pas alourdir l'utilisation du SCAE-CPC, les utilisateurs n'auraient pas l'obligation de renseigner de multiples informations ni lors de leur inscription, ni lors de l'ajout de documents. La conception et la présentation de celui-ci seront donc particulièrement soignées pour ne pas rebuter l'utilisateur.

### 3.2.2 Description des cas d'utilisation

#### 3.2.2.1 S'authentifier

- ☞ **Acteur principal** : Le personnel
- ☞ **Objectifs** : Se faire reconnaître par SCAE-CPC.
- ☞ **Préconditions** : L'interface d'authentification s'est affichée à l'écran

🔗 **Post-condition** : Le personnel a accès à l'espace de SCAE-CPC qui lui est réservée.

🔗 **Scenario nominal**

1. Le personnel saisit ses informations d'identification (nom d'utilisateur, mot de passe) dans les champs concernés.
2. SCAE-CPC vérifie la présence de l'un utilisateur détenant ces informations d'identification parmi les utilisateurs existants
3. SCAE-CPC lui affecte ses droits et ouvre l'espace qui lui est réservé.

🔗 **Alternatifs**

- (ia) Les informations saisies par l'utilisateur sont incomplètes.
  - SCAE-CPC notifie le personnel du manque d'information.
  - L'exécution reprend à l'étape i du scénario nominal.
- (iia) Les informations saisies par le personnel ne correspondent à aucun compte utilisateur SCAE-CPC notifie le personnel de l'inexistence d'un utilisateur ayant les identifiants saisies et propose au personnel de se créer un compte (voir le cas d'utilisation S'inscrire). L'exécution reprend à l'étape i du scénario nominal

### 3.2.2.2 S'inscrire

🔗 **Acteur principal** : Le personnel

🔗 **Objectifs** : Se créer un compte utilisateur SCAE-CPC.

🔗 **Préconditions** : Le personnel peut désormais se connecter dans SCAE-CPC

🔗 **Post-condition** : Le personnel a accès à l'espace de SCAE-CPC qui lui est réservée.

🔗 **Scenario nominal**

1. Le personnel saisit ses informations d'identification (nom d'utilisateur, mot de passe) dans les champs concernés.
2. SCAE-CPC vérifie la présence de l'un utilisateur détenant ces informations d'identification parmi les utilisateurs existants
3. SCAE-CPC vérifie la présence d'un utilisateur détenant ces informations d'identification (nom d'utilisateur, adresse email, mot de passe) parmi les utilisateurs existants
4. SCAE-CPC crée un compte utilisateur à ce personnel.

🔗 **Alternatifs**

- (ia) Les informations saisies par l'utilisateur sont incomplètes.

- SCAE-CPC notifie le personnel du manque d'information.
  - L'exécution reprend à l'étape i du scénario nominal.
  - (iia) Au moins une des informations d'identification (nom d'utilisateur, adresse email, mot de passe) saisies par le personnel converge déjà avec celui d'un compte utilisateur.
  - SCAE-CPC notifie le personnel de ce qu'un utilisateur inscrit détient déjà l'information convergeant avec celle qu'il a saisi et met en évidence cette information.
  - L'exécution reprend à l'étape i du scénario nominal
- L'exécution reprend à l'étape i du scénario nominal

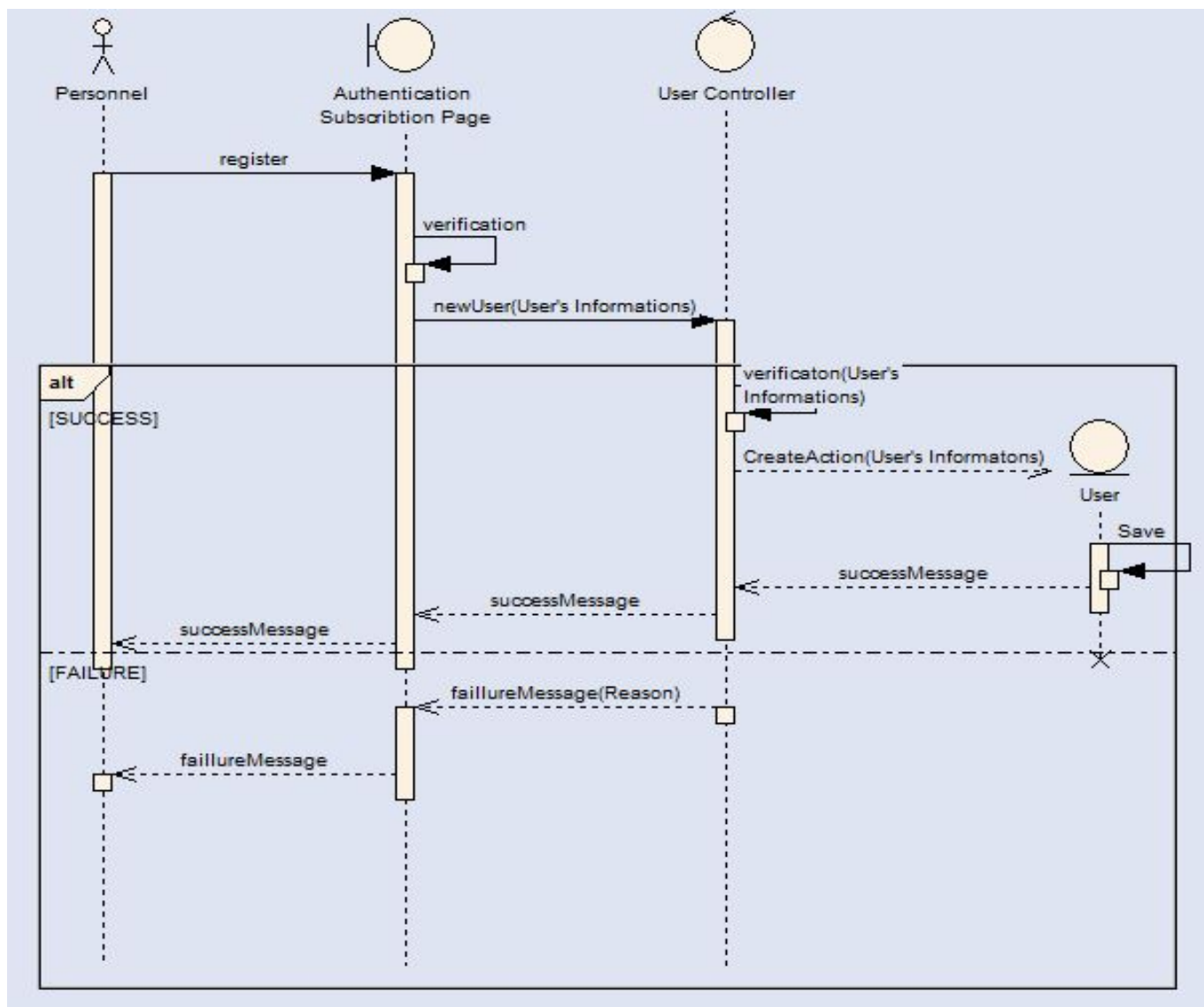


FIGURE 3.4 – Diagramme de séquences système de l'inscription d'un personnel

### 3.2.2.3 Sauvegarder un fichier

- ☞ **Acteur principal** : Le personnel
- ☞ **Acteur secondaire** : L'archiviste
- ☞ **Objectifs** : Le personnel désire sauvegarder permanemment un fichier..
- ☞ **Préconditions** : Le personnel s'est authentifié sur l'intranet (voir le cas d'utilisation S'authentifier).
- ☞ **Post-condition** : Le fichier téléchargé est chiffré et disponible pour les traitements par l'archiviste.

#### ☞ **Scenario nominal**

1. Le personnel télécharge un fichier, indique les informations (possesseur, type de document, titre, durée d'utilité administrative) sur le fichier et valide. D'autres informations telles que la date de création, le nom du fichier, l'emplacement, le département, sont automatiquement remplies par SCAE-CPC.<sup>8</sup>
2. SCAE-CPC vérifie la présence et la cohérence des informations données par le personnel.
3. SCAE-CPC collecte les informations sur le fichier, inscrit la date de création et l'auteur de la sauvegarde, chiffre symétriquement<sup>9</sup> le contenu du fichier avec la clé du département, ajoute la nouvelle sauvegarde constituée dans la file des sauvegardes à traiter par l'archiviste.
4. - SCAE-CPC notifie l'archiviste de la nouvelle sauvegarde.

#### ☞ **Alternatifs**

- (ia)- Le type de fichier n'est pas pris en compte par le SCAE-CPC. SCAE-CPC notifie le personnel de la non prise en charge du type de fichier et indique au personnel de compresser le fichier en archives zip avant de le télécharger.
  - SCAE-CPC notifie le personnel du manque d'information.
  - Le personnel remplit l'information.
  - SCAE-CPC continue les traitements tels que décrit à l'étape ii du scénario nominal.

### 3.2.2.4 Archiver un fichier

#### ☞ **Acteur principal** : L'archiviste

---

8. La date de création et l'auteur du document sont automatiquement inscrite pas SCAE-CPC. C'est une mesure de sécurité.

9. Le chiffrement symétrique a été évoqué dans l'Etat de l'art de ce mémoire

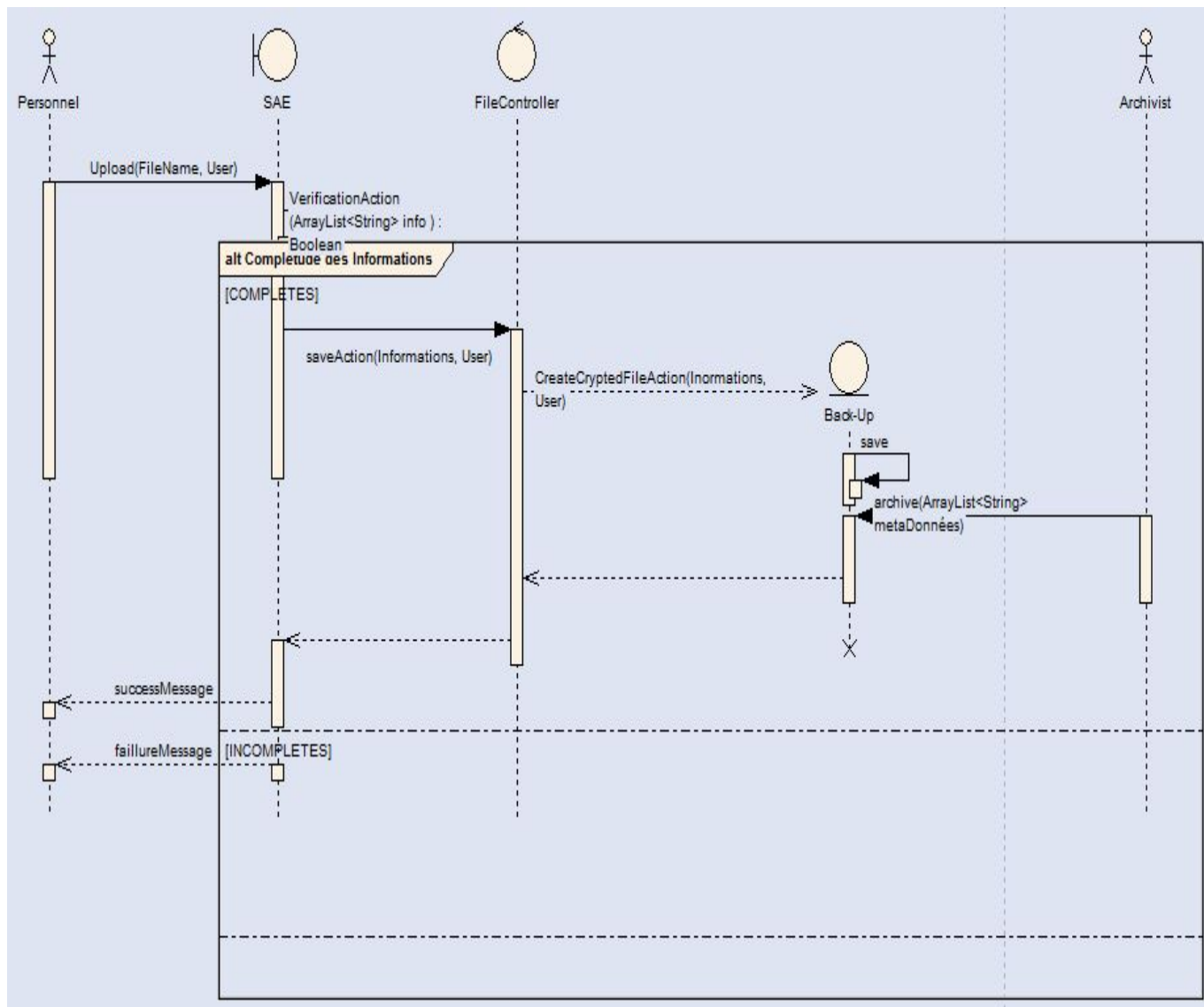


FIGURE 3.5 – Diagramme de séquences système de la sauvegarde d'un fichier

👉 **Acteur secondaire** : Le personnel

👉 **Objectifs** : L'archiviste traiter le cas d'un fichier qui lui a été soumis par le personnel.

👉 **Préconditions** : L'archiviste s'est authentifié sur l'intranet (voir le cas d'utilisation S'authentifier) et est notifié par SAC-CPC de la présence d'un fichier à traiter

👉 **Post-condition** : Le fichier sauvegardé fait désormais partir de l'arborescence des sauvegardes.

👉 **Scenario nominal**

1. L'archiviste complète les métadonnées sur le fichier (nom, index, le code,



commentaire).

2. L'archiviste sauvegarde les enregistrements effectués et positionne le fichier dans l'arborescence des sauvegardes.

#### ☞ **Alternatifs**

- (iia) L'archiviste détecte des informations inexactes sur le fichier à archiver parmi celles remplies par l'auteur du fichier.  
L'archiviste met à jour ces informations.

### 3.2.2.5 Chercher une archives

☞ **Acteur principal** : Le personnel (Qu'il soit l'archiviste ou tout autre personnel du CPC)

☞ **Acteur secondaire** : L'archiviste

☞ **Objectifs** : Le personnel veut trouver le plus rapidement possible un document précis dans l'ensemble du catalogue des archives. Il veut également pouvoir flâner comme il le ferait dans un vrai service d'archives et chercher des documents avec des critères variés.

☞ **Préconditions** : Le personnel s'est authentifié sur l'intranet (voir le cas d'utilisation S'authentifier) et le catalogue des archives est disponible

☞ **Post-condition** : Le personnel a trouvé l'archive précise qu'il cherchait, ou un dossier qui l'intéresse, voire plusieurs.

#### ☞ **Scenario nominal**

1. Le personnel lance une recherche rapide à partir de mots-clés : un objet, un titre, le nom d'un auteur, date de création, etc .
2. Le SAE affiche une page de résultat. Les dossiers sont classés par défaut par date de parution, le plus récent en premier.
3. Le personnel sélectionne un ouvrage.
4. Le SAE lui présente une fiche détaillée pour le dossier sélectionné.  
On y trouvera en particulier :
  - une image (pour la majorité des dossiers),
  - son titre, sous-titre, auteur(s), date de création, le nom du box dans les archives, nombre de documents
  - des éventuels commentaires sur ce dossier,

#### ☞ **Alternatifs**

- (ia) Le personnel n'a pas d'idée préconçue et préfère flâner dans les archives du CPC. Pour cela, le Système lui propose de le faire via l'explorateur de fichiers.  
Le personnel navigue dans ces pages et peut enchaîner sur l'étape 3 du scénario nominal.

- (ib) Le personnel (l'archiviste) choisit d'effectuer une recherche avancée.
  - Le personnel accède à un formulaire spécialisé lui permettant de combiner plusieurs types de recherche : par titre, auteur, possesseur, date de création, etc. Il peut également saisir directement le code de l'archive.
  - Le cas d'utilisation redémarre à l'étape 1 du scénario nominal.
- (iia) Le SCAE-CPC n'a pas trouvé d'ouvrage correspondant à la recherche. Le SCAE-CPC signale l'échec au personnel et lui propose d'effectuer une nouvelle recherche. Le cas d'utilisation redémarre à l'étape i du scénario nominal.
- (iib) Le SAE a trouvé de très nombreux dossiers.
  - Le SCAE-CPC signale le nombre d'ouvrages à au personnel et lui affiche une première page de résultats. Les autres pages sont accessibles directement ou par des symboles Suivante et Précédente.
  - Le personnel navigue dans ces pages et enchaîne éventuellement sur l'étape 3 du scénario nominal. Il peut également reclasser les ouvrages obtenus par différents critères : titre, auteur, etc.
- (iiia) Le personnel n'est pas intéressé par les résultats.
  - Le personnel revient à l'étape 1 du scénario nominal pour lancer une nouvelle recherche.
  - Le personnel abandonne la recherche. Le cas d'utilisation se termine en échec.

#### 3.2.2.6 Consulter une archive

👉 **Acteur principal** : Le personnel (Qu'il soit l'archiviste ou tout autre personnel du CPC)

👉 **Acteur secondaire** : Le chef service du département producteur de l'archive.

👉 **Objectifs** :Le personnel veut consulter une archive.

👉 **Préconditions** : Le personnel s'est authentifié sur l'intranet (voir le cas d'utilisation S'authentifier) et l'archives est disponible sur son espace.

👉 **Post-condition** :Le personnel accède aux contenu de l'archive.

👉 **Scenario nominal**

1. Le personnel procède à l'ouverture de l'archive.
2. Le SCAE-CPC vérifie les droit du personnel sur l'archive.
3. Le SCAE-CPC déchiffre et ouvre l'archive.

👉 **Alternatifs**

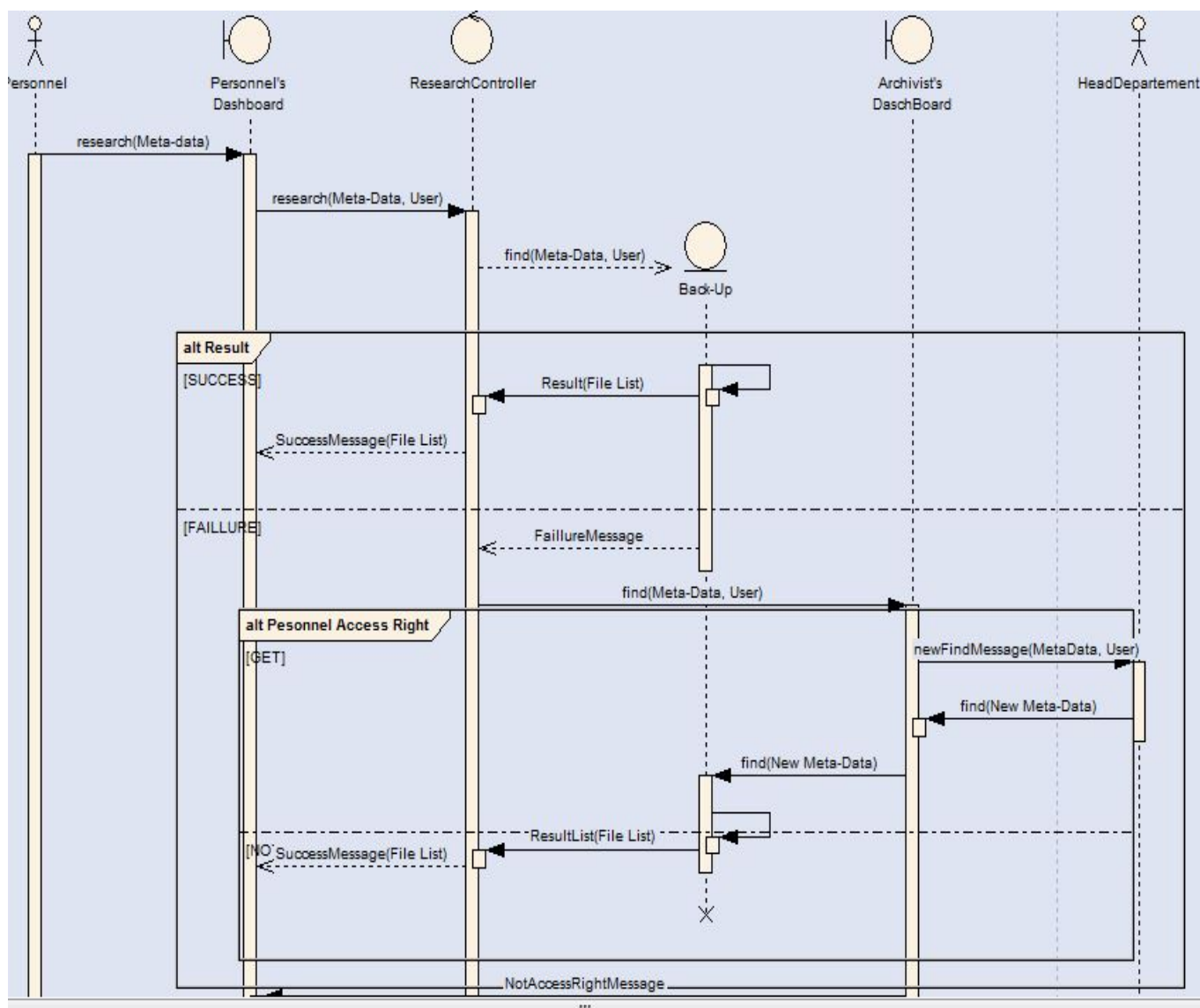


FIGURE 3.6 – Diagramme de séquences système de la recherche d’une archive

- (iia) Le personnel n’a pas le droit d’accéder au contenu du fichier du fait qu’il n’est pas du département source de ce fichier
- SCAE-CPC notifie le personnel de ce qu’il n’a pas le droit d’accès sur le fichier désiré et souligne la raison.
- Le personnel demande l’accès au contenu de cet archive a chef du département source.
- Le chef de département autorise au personnel l’accès en lecture à son archive.
- Le personnel consulte l’archive.

- (ja)- Le chef de département n'autorise pas l'accès à son archive au personnel ou ne réagit simplement pas.  
Le personnel ne peut simplement pas consulter l'archive.

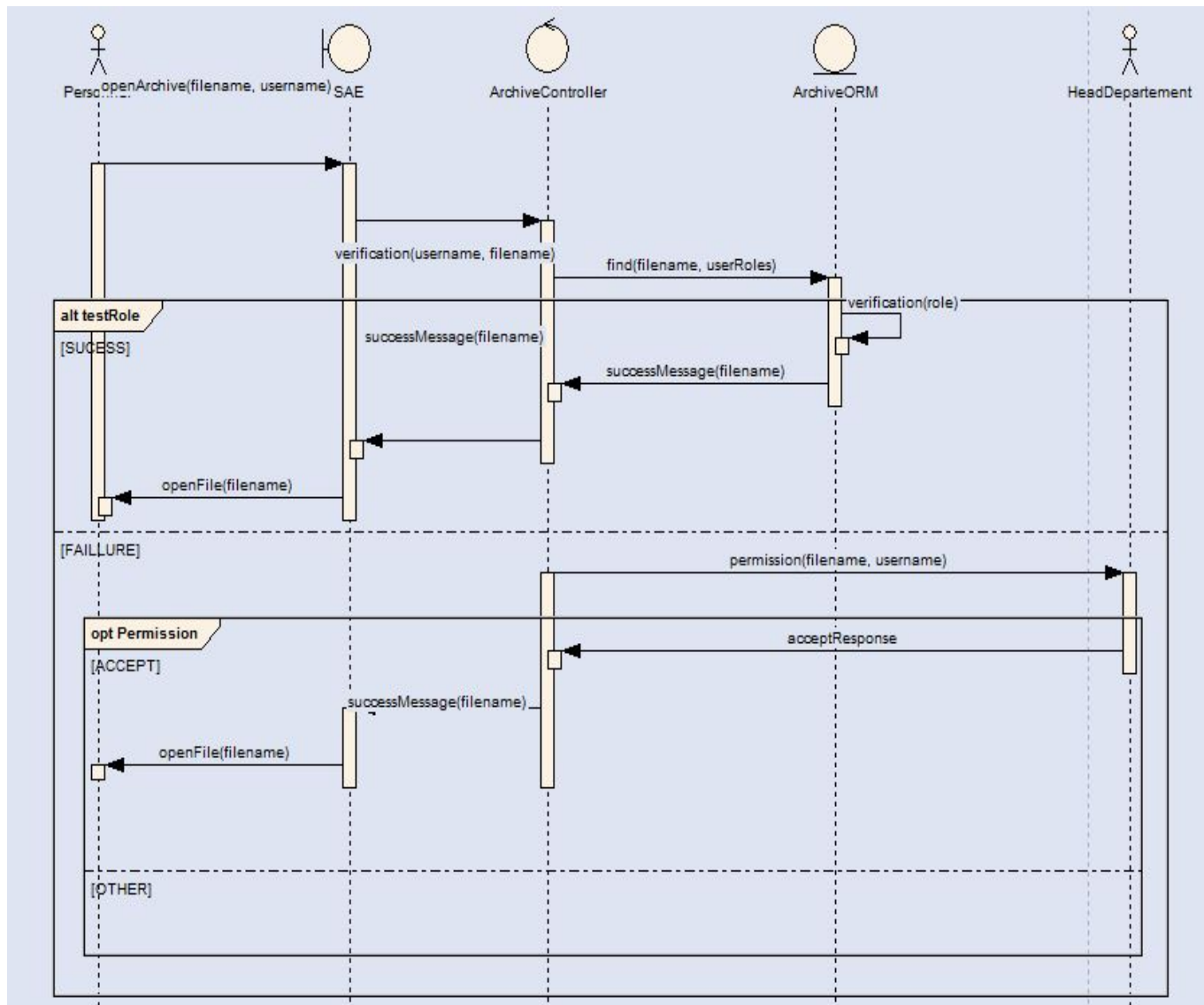


FIGURE 3.7 – Diagramme de séquences système de la consultation d'une archive

Les cas d'utilisation ci-dessus décrite de façon détaillée et schématique suffisent pour comprendre les fonctionnalités que doit offrir SCAE-CPC. La prochaine étape consiste en la conception de la solution telle que attendue par les utilisateurs auprès de qui les besoins ont été collectés. C'est l'objet de la partie suivante.

## SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD

### 3.2.3 Architecture de SCAE-CPC

SCAE-CPC se présente comme sur la figure 3.8 suivante :

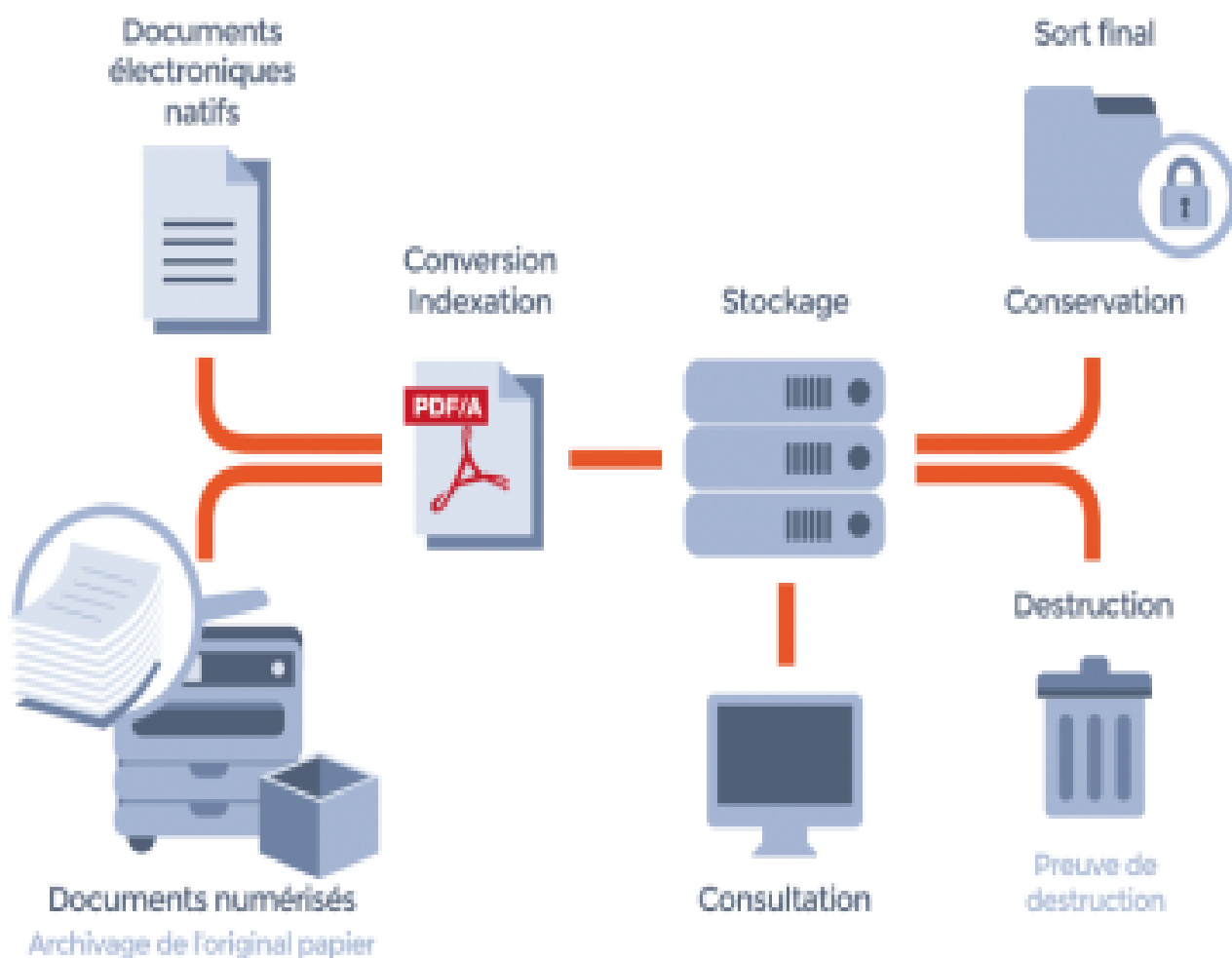


FIGURE 3.8 – Architecture de SCAE-CPC

Au module client :

1. les documents à archiver proviennent de diverses sources :
  - les fichiers conçus par le personnel ;
  - les documents physiques scannés ;
  - les fichiers produits par les logiciels utilisés au CPC (Optimaint, Glims, Sage ...)

2. L'utilisateur télécharge les fichiers et le SCAE-CPC chiffre les fichiers
3. L'archiviste se sert de SCAE-CPC pour constituer les sauvegardes. Au module serveur toutes les informations sur les sauvegardes constituées sont stockées et gérées par le SGBD. Les sauvegardes sont d'abord constituées localement. La DAO couplé SGBD facilitera les recherches d'archives.
4. Ces sauvegardes sont archivées par les services cloud ou détruits conformément à la politique d'archivage

### 3.2.3.1 Aspects de sécurité :

L'authentification est prise en charge par une composante principale de SCAE-CPC : *FosUserBundle* qui sera présentée dans le chapitre suivant. De même, elle gère les rôles (Administrateur, Chef département, Personnel) attribuées par l'administrateur aux utilisateurs. Vis à vis de la confidentialité et de l'intégrité, les fichiers sont déposés dans un serveur de fichiers sécurisé et dans un dossier protégé à l'accès et uniquement accessible aux propriétaires et gestionnaires de la ressource concernée. Notons que, une fois l'archivage effectué sur un fichier, celui-ci n'est plus modifiable.

Vis-à-vis de la disponibilité aux archives, ce point a été largement présenté dans le point I.5 du chapitre I : La politique d'archivage.

### 3.2.4 Diagramme de classes métiers

A partir des analyses précédentes, nous déduisons le diagramme de classes de conception ci-après : Il s'agit d'une description des classes et les packages du SCAE-CPC ainsi que les différentes relations entre celles-ci. Ce diagramme fait partie de la partie statique de notre modélisation UML car il fait abstraction des aspects temporels et dynamiques. Etant donné l'importance de la gestion des utilisateurs et de leurs droits sur les différents médias, il convient de répartir les entités en deux packages : User et Media. Les entités du package User sont reliées selon leur relations hiérarchiques et leur rôles, et les entités du package Media sont reliées selon les couches de regroupement des entités. A chacune des classes métiers, correspond une table de la base de données(BD). Cette BD est décrite dans la section suivante.

### 3.2.5 Modèle relationnel

La figure 3.10 ci-dessous représente le modèle logique de données sur lequel se fonde notre système de gestion de base de données(SGBD). Cette description structurée de nos données découlent du diagramme de classe de la figure 3.9 précédente. On y distingue les tables suivantes :

## SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD

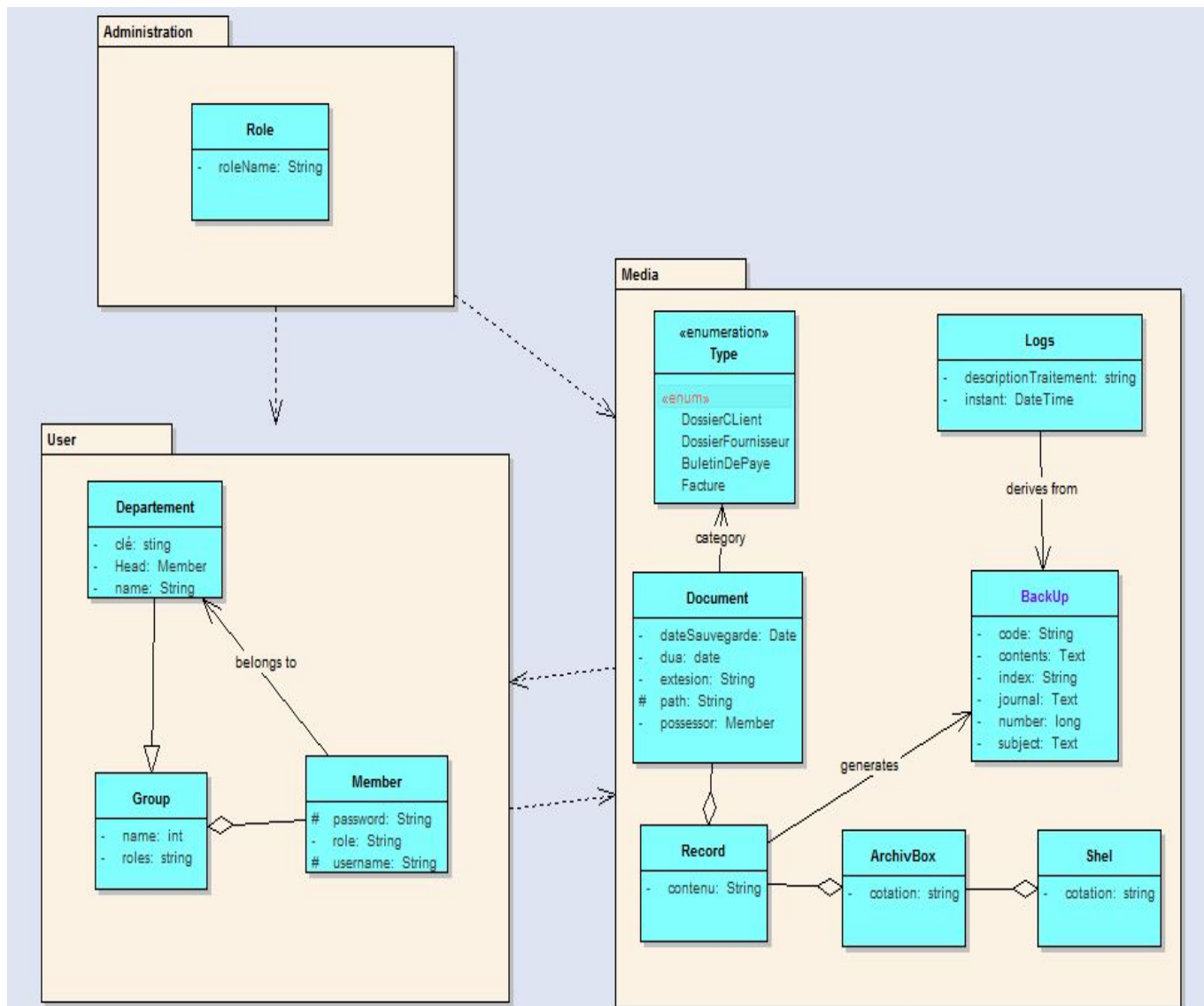


FIGURE 3.9 – Diagramme de classes métiers de SCAE-CPC

- ☞ La table Member enregistre les informations sur le personnel de SCAE-CPC ;
- ☞ La table Role liste les rôles créés dans SCAE-CPC ;
- ☞ La table RoleMember enregistre les attributions de rôles au personnel ;
- ☞ La table Departement liste les informations sur départements au sein desquels le personnel exerce ;
- ☞ La table Document liste les métadonnées des documents destinés à l'archivage ;
- ☞ La table Type est l'énumération des différents types de documents traités par SCAE-CPC ;
- ☞ La table Record liste les dossiers dans lesquels les documents archivés sont rassemblés ;

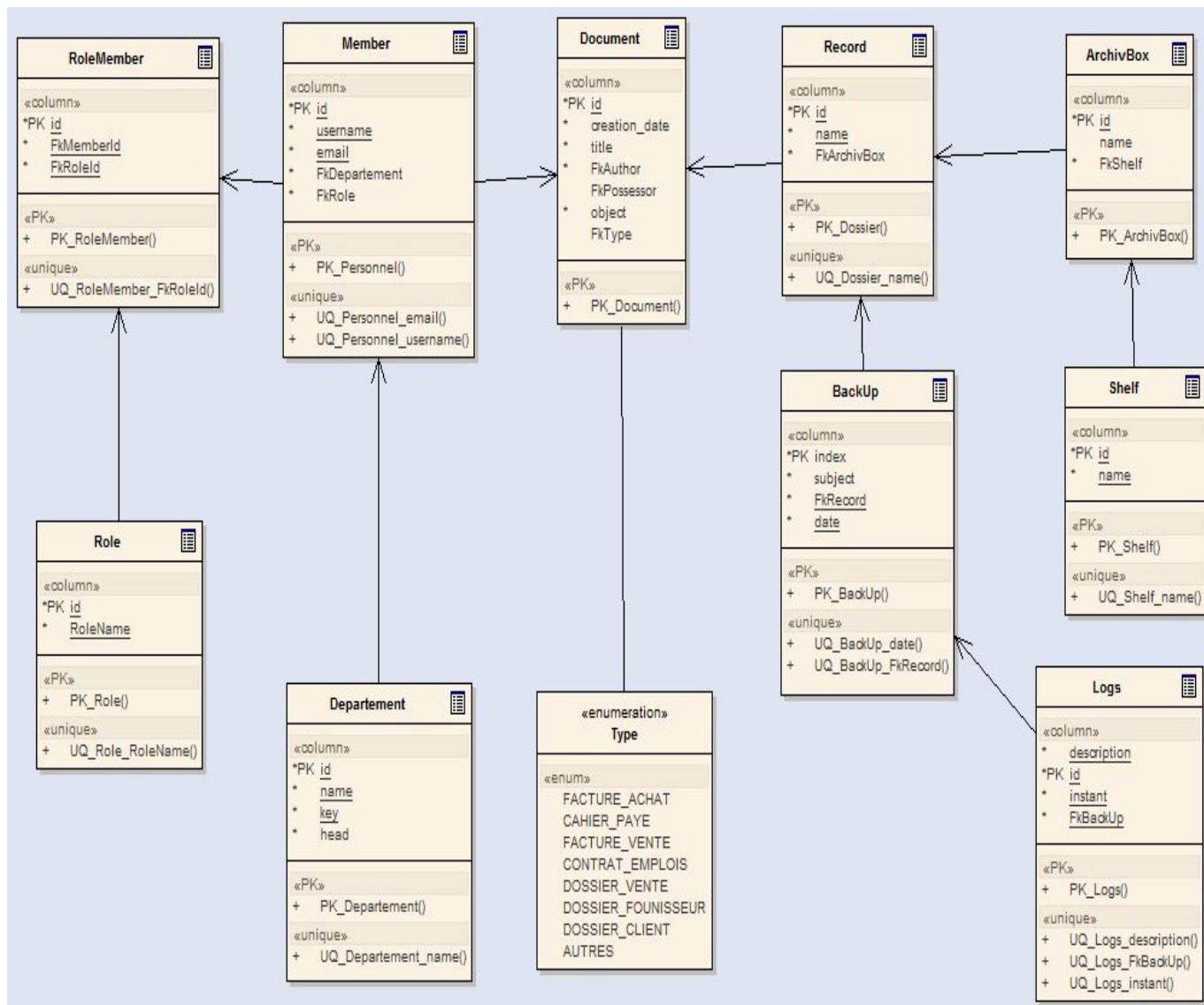


FIGURE 3.10 – Modèle logique de données de SCAE-CPC

- ☞ La table ArchiveBox liste les informations sur les box d'archives au sein desquels sont rassemblés les dossiers ;
- ☞ La table Shelf liste les rayons des archives ;
- ☞ La table BackUp liste les informations sur les sauvegardes générées dans le processus d'archivage ;
- ☞ Et la table Logs enregistre les opérations effectuées sur les sauvegardes.



### 3.2.6 Les diagrammes d'états-transitions

Une machine à état spécifie les séquences d'états qu'un objet peut parcourir durant sa vie en réponse aux événements qui lui adviennent, ainsi que les réactions correspondantes. Toutes les classes du modèle statique ne requièrent pas nécessairement une machine à états, représentée par un diagramme d'états. Il s'agit donc de trouver celles qui ont un comportement dynamique complexe nécessitant une description. Des entités existantes, l'entité Fichier est la plus dynamique. Il convient d'illustrer ces changements à l'aide d'un automate fini, celui de la figure 3.11 suivante.

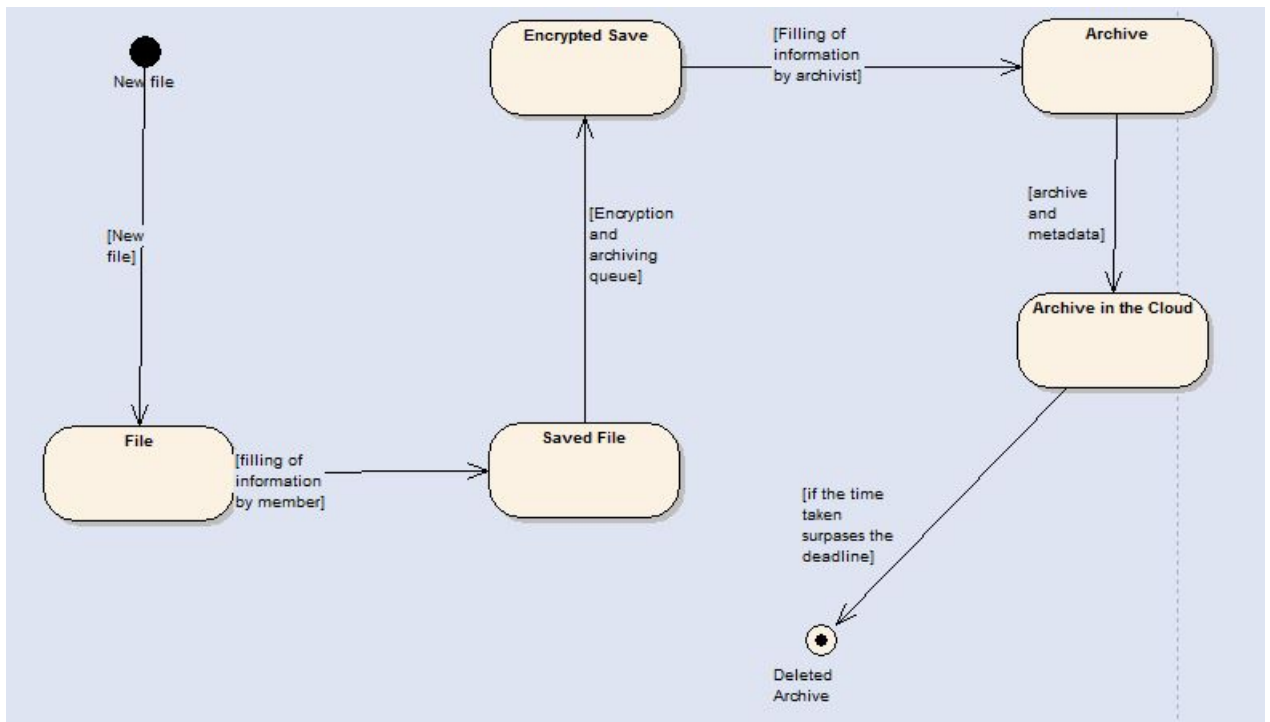


FIGURE 3.11 – Architecture technique

### 3.2.7 Diagramme d'états-transitions de l'entité Fichier

Tout fichier à archiver doit se voir associer des métadonnées au niveau du personnel, ensuite son contenu sera chiffré et soumis au traitement de l'archiviste, une fois traité, il fait partir des sauvegardes qui seront archivées dans le Cloud par le prestataire.

*Il a été question dans ce chapitre de présenter les besoins exprimés par les destinataires de SCAE-CPC, analyser ces besoins et concevoir notre SCAE-CPC, étape ultime avant la mise en œuvre. A travers une architecture modulaire telle que recommandée par la méthode Unified Process (UP) nous avons été capables de définir et de décrire l'aspect conceptuel de SCAE-CPC.*

- ☞ Editeur en couleur ;
- ☞ Gestion des projets multi-langage ;
- ☞ Refactorisation ;
- ☞ Editeur graphique d'interfaces et de pages Web ;
- ☞ Débogage complet basé sur Xdebug ;
- ☞ Intégration native de certains Frameworks ;
- ☞ Auto complétion de méthodes et documentation sur les méthodes en question ;

# 4

## IMPLÉMENTATION ET RÉSULTATS

---

Dans ce chapitre, sont présentés les éléments liés à l'implémentation de notre solution logicielle, en l'occurrence les outils utilisés ainsi que leur contexte d'utilisation. Par la suite, nous présenterons quelques résultats obtenus accompagnés de commentaires.

### Sommaire

---

<b>4.1</b>	<b>Choix des outils</b>	<b>42</b>
4.1.1	Langages de programmation et Integrated Development Environment (IDE)	42
4.1.2	Symfony 2	42
4.1.3	BOOTSTRAP 3.0 /FLAT UI DESIGN/MATERIAL-DESIGN	42
4.1.4	Twig	43
4.1.5	Doctrine	44
4.1.6	API de traitement	44
4.1.7	Les bundles	44
<b>4.2</b>	<b>Implémentation</b>	<b>45</b>
4.2.1	Diagramme de packages	45
4.2.2	Diagramme de déploiement	45
<b>4.3</b>	<b>Résultats</b>	<b>47</b>

---

## 4.1 Choix des outils

Dans le soucis de facilité l'évolution et d'obtenir de bon rendement dans les opérations effectuées au sein de notre système, nous avons sélectionnés des outils en fonction de leur popularité, de la facilité de leur utilisation au cours du développement et de leur interopérabilité.

### 4.1.1 Langages de programmation et Integrated Development Environment (IDE)

Comme langage de programmation, nous avons opté pour le PHP(2) version 5. En effet, cette version offre tous les avantages liés à l'utilisation de la programmation orientée objet (héritage, polymorphisme, système d'interface...). Nous avons choisi Netbeans comme environnement de développement de notre application web. En effet, dans sa version (8.0.2), Netbeans nous offre un très bon support pour le développement d'applications web PHP. Il nous offre surtout l'auto complétion dont nous avons besoin pour développer avec le Framework Symfony 2.

### 4.1.2 Symfony 2

Symfony, version 2.8 est un Framework MVC (kit de logiciel basé sur le Modèle Vue Contrôleur) français, libre, écrit en PHP5 et sorti le 28 juillet 2011. Il permet de développer, rapidement et avec facilité, des sites et applications Web (il faut tout de même avoir les bases des différents langages utilisés tels que le HTML, CSS, JQuery JavaScript ou PHP). Le code de SCAE-CPC est divisé en trois couches :

- ☞ La couche Modèle : ce que SCAE-CPC est capable de faire ;
- ☞ La couche Vue : ce avec quoi l'utilisateur interagit ;
- ☞ La couche Contrôleur : ce qui gère les événements afin de mettre à jour la vue ou le modèle.

Symfony permet l'utilisation de templates PHP et Twig ; ce qui allège grandement le code. Il est très modulable, car il peut être couplé à un grand nombre de plugins.

### 4.1.3 BOOTSTRAP 3.0 /FLAT UI DESIGN/MATERIAL-DESIGN

Bootstrap est une api permettant d'habiller la partie visible par l'utilisateur d'une page web. C'est un projet open source initié en 2010 par deux développeurs travaillant chez Twitter qui a connu beaucoup de succès. Par la suite plusieurs développeurs intégrés le projet. Il est basé sur du CSS qui d'avoir un système de grilles intéressant pour la mise en forme du site, des différentes typographies, une mise en forme des tableaux, de jolis boutons etc. Il possède également des composants que l'on peut intégrer à nos

## SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD

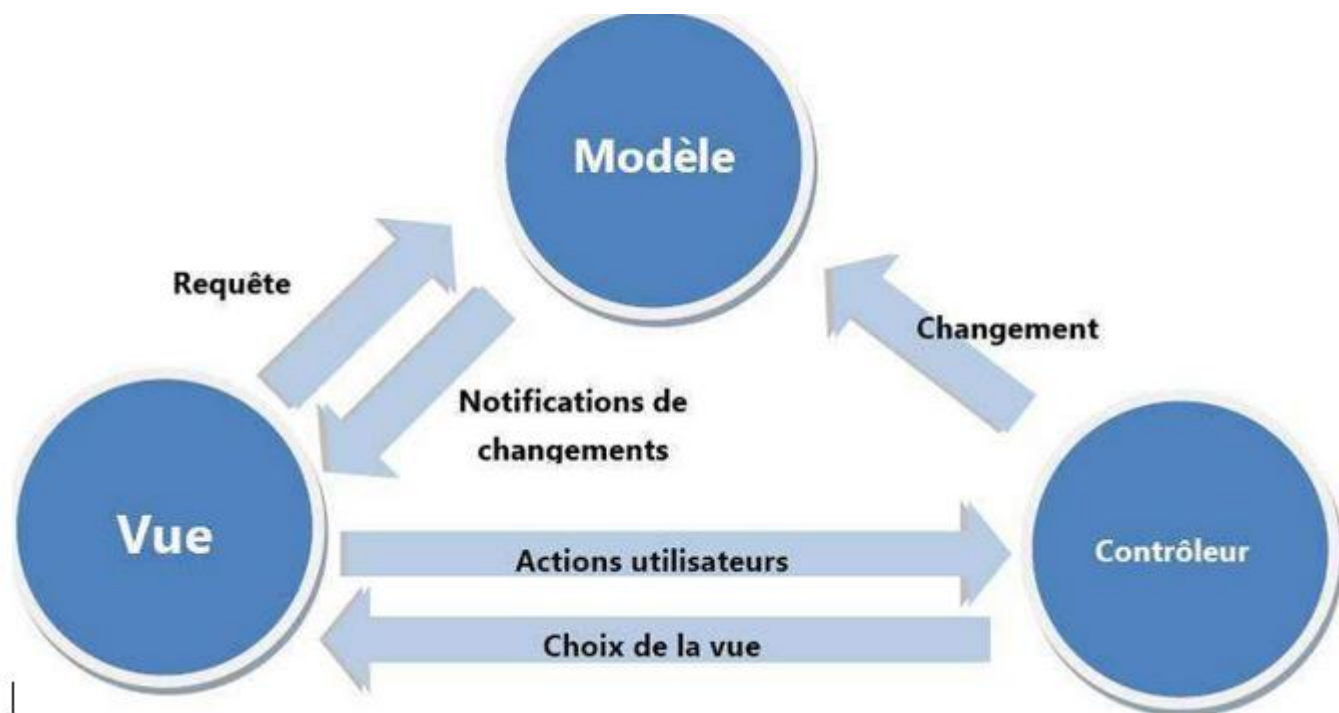


FIGURE 4.1 – Architecture MVC

pages (barre de navigation/progression, pagination...), du JavaScript pour dynamiser la page et enfin du jQuery. Flat-ui design et material-design sont des api d'habillage dérivant de bootstrap avec des spécificités bien définies.

#### 4.1.4 Twig

Twig est un moteur de Template<sup>1</sup> PHP permettant de séparer la couche présentation des applications web, tout en gardant flexibilité, rapidité et facilités au développement. Twig offre un certain nombre d'avantages aux développeurs :

- ☞ **Rapidité** : Twig compile le code des templates en des codes PHP bien plus optimisés. Le superflu de code par rapport au PHP ordinaire est réduit à son strict minimum ;
- ☞ **Sécurité** : Twig donne la possibilité au développeur de paramétrer le code afin qu'il puisse s'exécuter dans une Sandbox, ce qui permet à l'utilisateur qui utilise l'application de n'avoir accès qu'à un nombre limité de ressources. Il donne aussi la possibilité d'activer automatiquement l'échappement des caractères
- ☞ **Flexibilité** : Le développeur peut facilement étendre Twig afin de satisfaire des exigences particulières.

1. Les moteurs de templates sont les outils utilisant les templates pour en générer les fichiers textes

#### 4.1.5 Doctrine

Doctrine est une ORM<sup>2</sup>, c'est-à-dire est une classe (ou bien plus souvent un ensemble de classes) visant à ce que l'utilisateur puisse manipuler ses tables de données comme si c'étaient des objets. Il permet le mapping entre le modèle objet et le modèle relationnel en tenant compte des concepts tels le polymorphisme, l'agrégation, l'héritage. Une caractéristique de Doctrine est le faible niveau de la configuration qui est nécessaire pour démarrer un projet. Doctrine peut générer des classes d'objets à partir d'une base de données existante, et le programmeur peut alors préciser les relations et ajouter des fonctionnalités personnalisées aux classes générées. Il n'est pas nécessaire de générer ou de maintenir des schémas XML complexes, comme dans de nombreux autres Framework. Une autre caractéristique clé de Doctrine est la capacité à écrire des requêtes de bases de données dans un langage orienté objet DQL<sup>3</sup>. Sinon, optionnellement, la classe QueryBuilder permet de construire des requêtes via une interface fluide. Ces interfaces fournissent aux développeurs des puissantes alternatives à SQL<sup>4</sup>, en leur offrant la possibilité de changer de base de données, sans nécessiter de duplication de code.

#### 4.1.6 API de traitement

Nous avons précédemment présenté les API utilisées pour l'affichage du côté client, il sera question dans la suite de faire un briefing de quelques API utilisées pour les traitements côté serveur.

#### 4.1.7 Les bundles

Un bundle peut être simplement compris comme une brique de l'application. Symfony2 utilise ce concept novateur qui consiste à regrouper dans un même endroit, le bundle, tout ce qui concerne une même fonctionnalité. Ainsi dans le cadre de notre application, nous nous sommes servis des bundles. En voici quelques.

- ☞ **FosUserBundle** : La gestion utilisateur est le cœur de notre application web. FosUserBundle est un kit recommandé depuis la page de Symfony. Il intègre aussi les mécanismes configurables de gestion des utilisateurs.
- ☞ **DoctrineFixtureBundle** : L'utilisation des capacités de Doctrine à générer des données pour alimenter une base de test requiert cette extension.
- ☞ **SonataUserBundle** : compatible avec FosUserBundle offre une interface d'administration des utilisateurs

---

2. Object-Relational Mapping

3. Doctrine Query Language

4. Structured Query Language

- ☞ **Aws-SDK-Php** : est une bibliothèque PHP moderne et à code source libre qui facilite l'intégration de votre application PHP aux services AWS tels qu'Amazon S3, Amazon Glacier et Amazon DynamoDB
- ☞ **KnpgaufretteBundle** : Gaufrette est une librairie PH 5.3 ou plus offrant une abstraction du système de fichiers. Cette couche d'abstraction nous permet de développer des applications sans connaître où et comment seront stockés les fichiers media.
- ☞ **KnpmenuBundle** : brique maitresse qui organise SCAE-CPC et permet aux utilisateurs de naviguer.
- ☞ **SonataAdminBundle** : Offre une interface d'administration des utilisateurs.
- ☞ **SonataDoctrineORMAdminBundle** : Intègre la couche Doctrine ORM dans SonataAdminBundle

## 4.2 Implémentation

Une fois le choix des outils décrits, il convient à présent de procéder à l'implémentation proprement dite de notre solution. Cela sera fait à l'aide du diagramme de packages et le diagramme de déploiement !

### 4.2.1 Diagramme de packages

Ce diagramme représente la répartition physique (sur disque) des différents paquets du projet, il présente aussi les interactions entre les éléments des différents paquets. Les packages sont conçus de manière à maximiser la cohérence interne (les éléments du même package doivent être cohérents), et à minimiser le couplage externe (le package ne doit pas dépendre trop des autres packages). Le code de SCAE-CPC est organisé en 3 packages majeures :

**ArchivesMediaBundle** : qui rassemble les entités et traitements relatifs aux traitements des archives.

**ArchivesUserBundle** : qui rassemble les entités portant sur la gestion des utilisateurs

**ApplocationSonataAdminBundle** : qui porte sur l'administration du SCAE-CPC.

### 4.2.2 Diagramme de déploiement

En UML, un diagramme de déploiement est une vue statique qui sert à représenter l'utilisation de l'infrastructure physique par le système et la manière dont les

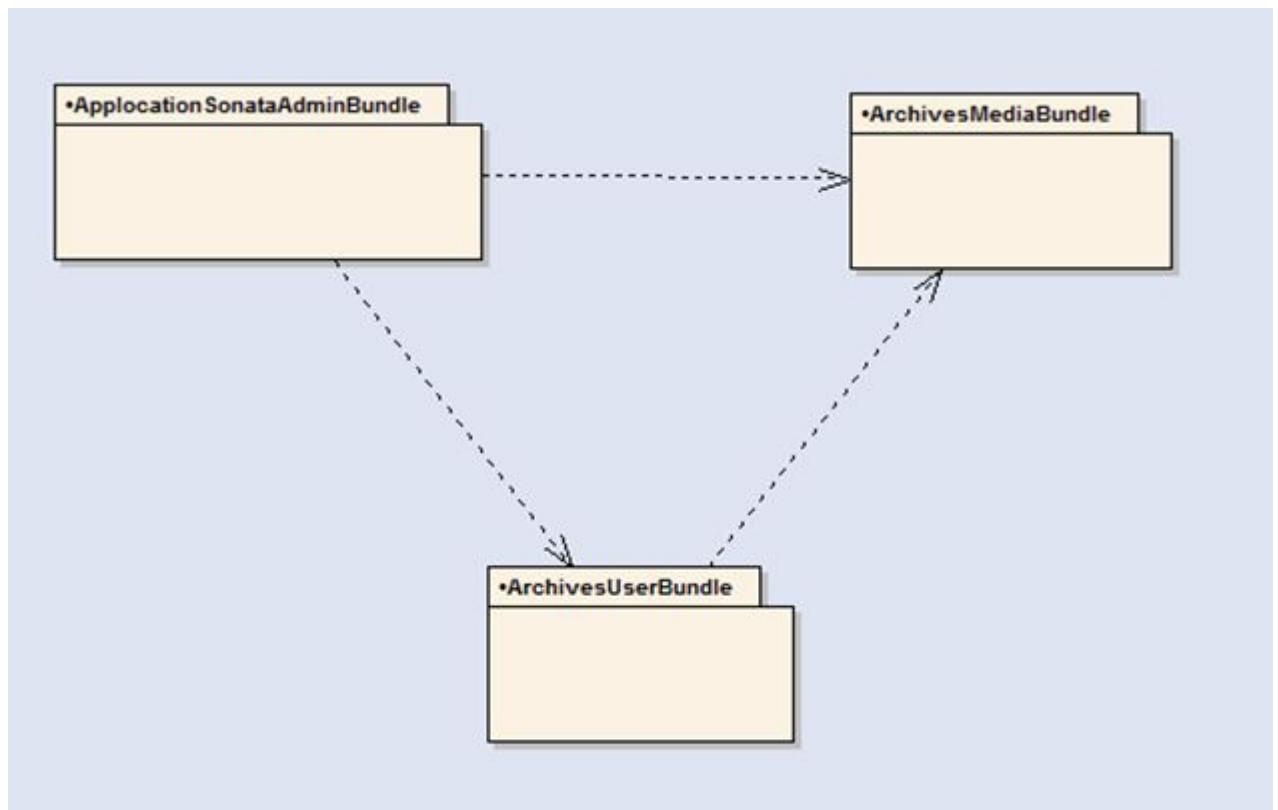


FIGURE 4.2 – Diagrammes de packages

composants du système sont répartis ainsi que leurs relations entre eux. L'architecture mise en place dans SCAE-CPC est une architecture 3-tiers. Nous avons :

- le tiers du client qui est essentiellement constitué par le navigateur web client à partir duquel il accède à l'application par le protocole http ;
- le tiers du serveur web qui est celui qui héberge les codes sources de notre application web développée sous Symfony 2 ;
- le tiers du serveur de données qui est constitué par l'instance de notre base de données MySQL. C'est ce qui est décrit dans la figure ci-dessus.



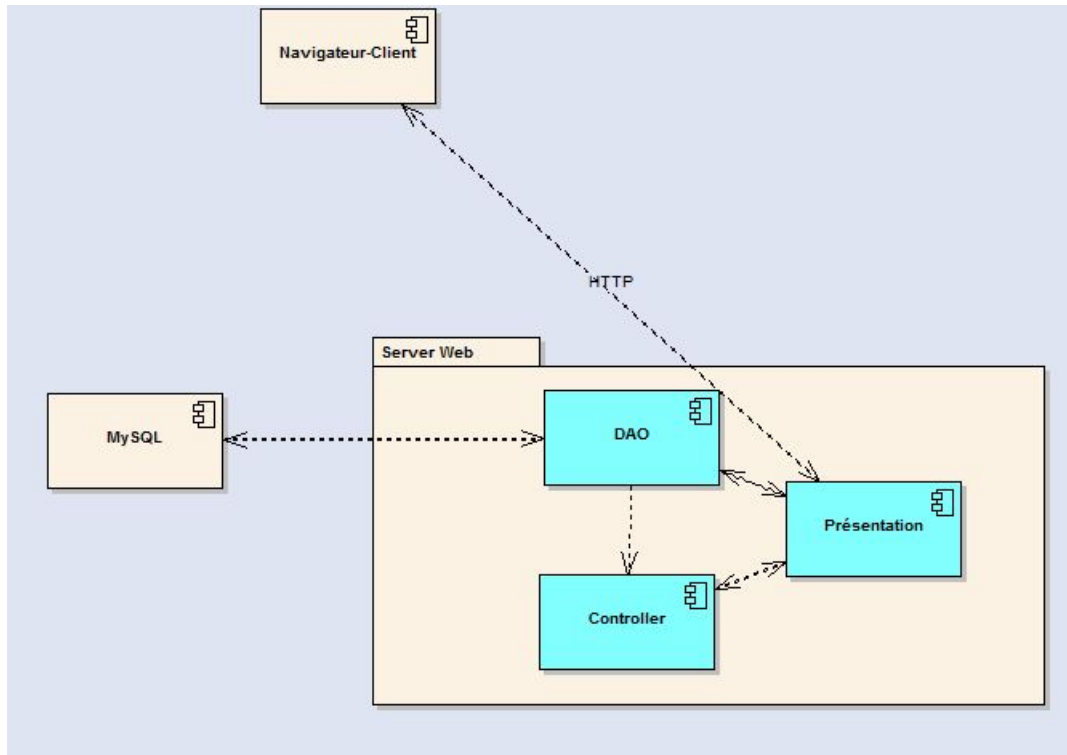


FIGURE 4.3 – Diagrammes de packages

### 4.3 Résultats

Nous nous proposons ici de présenter un scénario donnant un aperçu de la manière dont le processus de l'archivage se passe à travers SCAE-CPC. Le scénario commence par l'inscription, suivie de la connexion de l'administrateur informatique. Par défaut, ce personnel a jouit des privilèges de simple personnel dans SCAE-CPC, à moins que l'administrateur lui octroie un rôle plus élevé<sup>5</sup>(figure) . Le membre du personnel peut télécharger<sup>6</sup> un fichier, ajouter les informations attendues dans les champs (figure) ). Une fois soumis le fichier est symétriquement chiffré et parvient comme sauvegarde dans la file d'attente du poste de l'archiviste (Figure). Ce dernier ajoute à la sauvegarde

5. Nous rappelons qu'il existe 4 rôles dans l'application. Par ordre de privilège croissant, il s'agit de :

- ☞ **La fonction de personnel** : tout personnel du Centre pasteur a la possibilité de soumettre ses documents électroniques aux service des archives via SCAE-CPC. Il pourra les consulter aussi.
- ☞ **La fonction de chef de département** : Celui-ci, en plus d'être utilisateur, sert aussi d'intermédiaire entre deux départements et peut autoriser au refus de la consultation d'une archive par un personnel d'un autre département.
- ☞ **L'archiviste** : Ce rôle est celui du responsable de la l'enregistrement des documents soumis au service des archives.
- ☞ **l'administrateur** : Ce rôle revient au responsable du service informatique et tout autre administrateur sous la responsabilité duquel il travaille.

6. Télécharger dans le sens de l'upload

# SCAE-CPC : INSCRIPTION

( PRECISEZ INFORMATIONS DEMANDEES! )

**Nouvel utilisateur?**

**Username**

- The username is already used

**Email**

- The email is already used

**Password** .....

**Verification** .....

**Département**

FIGURE 4.4 – Page d’inscription de SCAE-CPC

les informations (code, dossier). L’administrateur ayant paramétré les configurations du serveur Cloud, SCAE-CPC envoie un exemplaire des sauvegardes périodiquement.

Sur cette figure 4.4 , le personnel de la cellule informatique Amougou se crée un compte.

# SCAE-CPC : LOGIN

( Connectez-vous pour bénéficier des fonctionnalités )

**Entrez vos paramètres de connexion**

**nom utilisateur ou email**

**mot de passe**

☐ se souvenir de moi

**valider**

FIGURE 4.5 – Page de connexion de SCAE-CPC

Sur la figure 4.5 l'administrateur informatique se connecte dans SCAE-CPC.

<input type="checkbox"/>	Username	E-Mail-Address	Groups	Enabled	Locked	Created at	Imperso
<input type="checkbox"/>	admin2	fopoar2@gmail.com	Informatique	yes	no	July 16, 2017 00:08	-
<input type="checkbox"/>	Mboh Alain	alainmboh@gmail.com	GRH	yes	no	July 16, 2017 07:03	-
<input type="checkbox"/>	NGNAWE Jonas	jonas@yahoo.com		yes	no	July 16, 2017 07:05	-
<input type="checkbox"/>	Dr eppoh valere	valere@yahoo.com	DAAF	yes	no	July 16, 2017 07:06	-
<input type="checkbox"/>	Atangana	atangana@yahoo.com	GRH	yes	no	July 16, 2017 07:07	-
<input type="checkbox"/>	amougou	amougou@gmail.com		yes	no	July 17, 2017 07:18	-
<input type="checkbox"/>	All elements (6)		Delete ▼	OK	Download ▼ - 1 / 1 - 6 results - Pe		

FIGURE 4.6 – Liste des utilisateurs de SCAE-CPC

Sur la figure 4.6 l'administrateur a la possibilité de consulter la liste des utilisateurs.

Edit "NGNAWE Jonas"

User

Security

Status

☐ Locked

☐ Expired

☒ Enabled

☐ Credentials expired

Groups

Groups

☐ Informatique

☐ DAAF

☒ Archives

☐ GRH

Add new

FIGURE 4.7 – Edition de role dans SCAE-CPC, cas de Jonas

Sur la figure 4.7, il affecte l'utilisateur Jonas au département des archives et lui affecte le role d'archviste.

SYSTEME CRYPTOGRAPHIQUE POUR ARCHIVAGE ELECTRONIQUE EN CLOUD

Mémoire présenté par FOKAM POKA ARSENE

P. 51

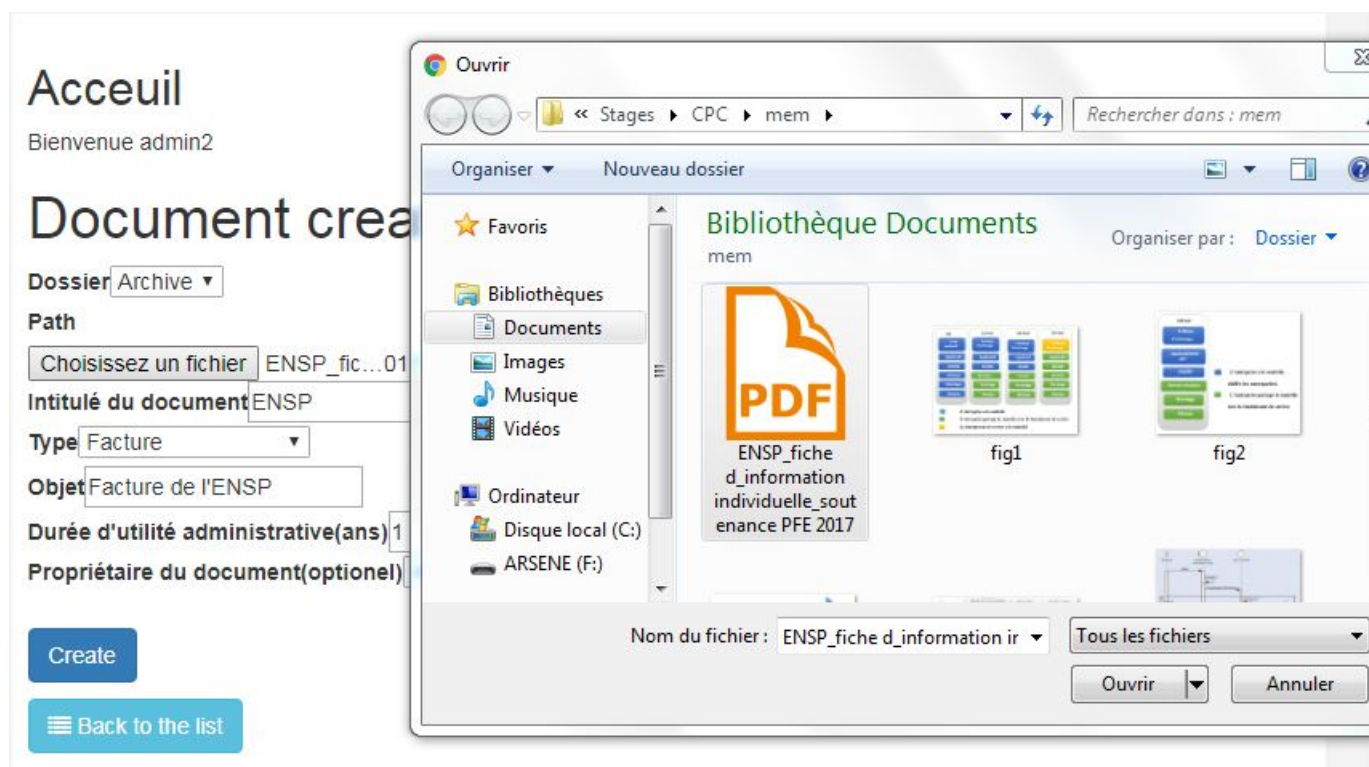


FIGURE 4.8 – Création d'une nouvelle sauvegarde

La création d'une sauvegarde passe par l'upload du fichier et l'édition des propriétés côté utilisateurs simple.(Figure 4.8)

<input type="checkbox"/>	list.label_code	list.label_name
<input type="checkbox"/>		fig1.JPG
<input type="checkbox"/>		fig1.JPG
<input type="checkbox"/>		fig1.JPG
<input type="checkbox"/>		COMMUNIQUÉ de Soutenance.pdf
<input type="checkbox"/>		ENSP_fiche d_information individuelle_soutenance PFE 2017.pdf
<input type="checkbox"/>	All elements (5) <div>Delete <input type="button" value="OK"/></div>	
<div><input type="button" value="Download"/></div>		

FIGURE 4.9 – Liste des sauvegardes

Dans la figure 4.9, l'archiviste peut consulter la liste des documents archivés.

Bienvenue admin2

## Document archivage

Code

Intitulé du document


Type

Titre

Objet

Possessor

Dossier

 Archiver



 Back to the list  Delete

FIGURE 4.10 – Archivage d'un document

L'archivage proprement dit consiste pour l'archiviste à affecter un code, logger le document dans un dossier.(Figure 4.10)



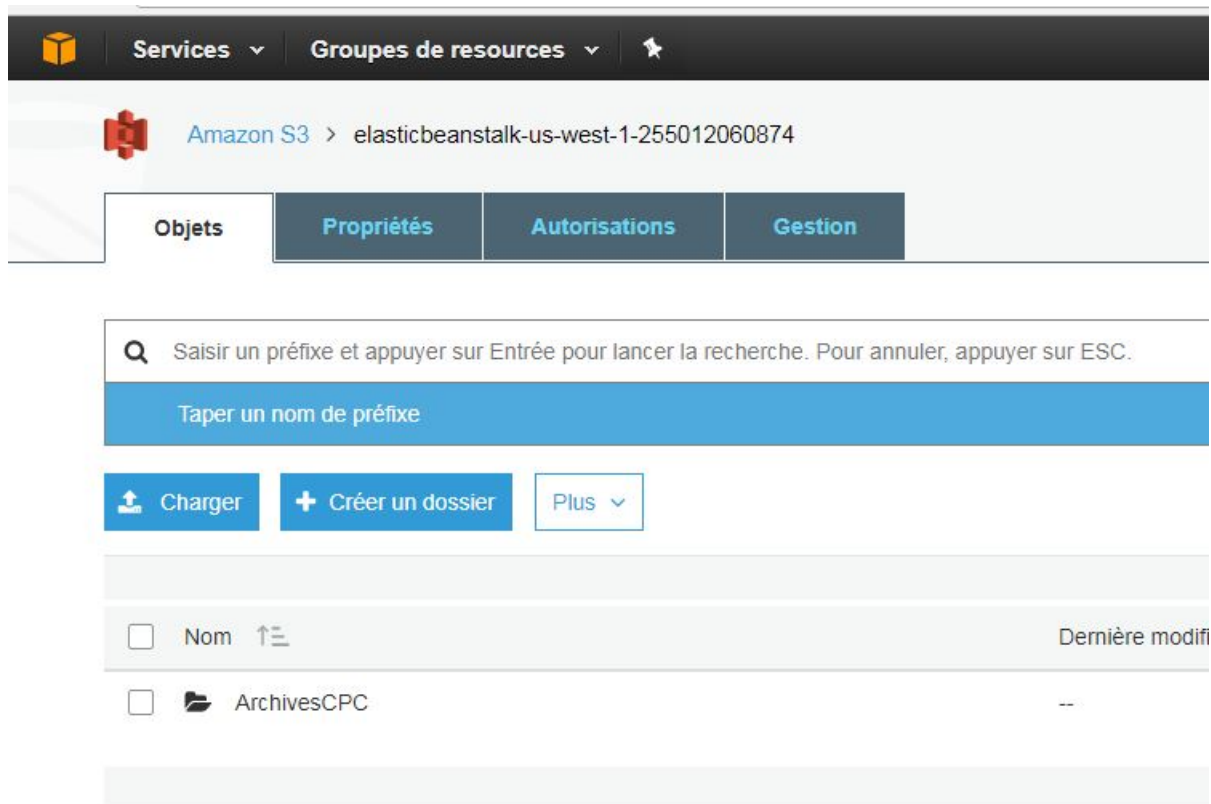


FIGURE 4.11 – Archivage d'un document

Après configuration par l'administrateur informatique, le répertoire des archives est simplement copié dans le bucket<sup>7</sup> chez le prestataire Amazone. Une capture de ce bucket est représentée sur la figure 4.11.

---

7. Unité de stockage dans Amazone

# CONCLUSION GENERALE

---

Ce travail portait sur la mise en place d'un Système Cryptographique d'Archivage Electronique au Centre Pasteur du Cameroun. Il était question de proposer une solution de dématérialisation des archives qui permettra de préserver la sécurité des archives. Suivant une démarche précise et respectueuse des méthodologies en matière de gestion des projets, nous avons défini une chaîne d'activités consistant tout d'abord à l'élaboration et à l'adoption d'une politique d'archivage, au recueil des besoins auprès du personnel, à l'analyse de ces besoins, à la conception de SCAE-CPC, à son implémentation et à la validation des résultats. Tous ces éléments sont orchestrés grâce à une architecture qui allie simplicité et efficacité. Plusieurs axes d'améliorations subsistent. Notamment au niveau de l'amélioration de composants utilisés durant l'implémentation, car les routines mises en œuvre connaissent des mises à jours fréquentes. D'autre part, nous imposons aux utilisateurs de numériser les archives physiques actuelles avant de les soumettre à l'archivage. Afin de transposer peu à peu à une gestion numérique complète de la chaîne des activités au CPC, il est nécessaire de réviser l'interface entre SCAE-CPC et les autres applications intervenant dans cette chaîne. Mais cela est aussi dépendante des habitudes du personnel et des clients du CPC. Dans tout projet de gestion électronique des documents (GED), la difficulté majeure réside dans l'analyse du processus. Il faut analyser le périmètre des documents, les besoins des parties prenantes du projet avant de donner une quelconque orientation à la solution. Après avoir bien défini le processus, il faut faire des choix techniques. A la fin, nous avons encore enchaîné avec la prise en main de LaTeX en vue de la rédaction de ce mémoire.

Ce stage au CPC nous a donné de faire une connaissance profonde de la GED et de nous familiariser aux principes de l'archivistique. Il nous a permis en tant qu'acteur principal de ce projet, d'assumer la responsabilité en un domaine capital du fonctionnement d'une entreprise. Les retombées sur le plan technique sont sans doute indéniables, vu la diversité des outils et des technologies (Symfony2, Doctrine) auxquelles nous découvrons et maîtrisons pour la réalisation de ce travail. Par ailleurs ce stage nous a permis de développer des qualités sur le plan humain telle l'écoute, l'ouverture et l'humilité pour ne citer que celles-ci.

# REFERENCE

---

## BIBLIOGRAPHIE

I	<b>L'ASSEMBLEE NATIONALE</b> ; Loi N° 2000/010 du 19 décembre 2000 régissant les archives ; 2000
II	<b>L'ASSEMBLEE NATIONALE</b> ; Loi N° 2000/010 du 19 décembre 2000 régissant les archives ; 2000
III	<b>GABAY (Joseph) , GABAY(David)</b> UML2 Analyse et Conception Dunod 2008
IV	<b>MANI (Serges Flavien)</b> ; Sécurité Informatique Chapitre 2 Protocoles et Cryptographie, 2016
V	<b>OHADA</b> ; Acte uniforme révisé relatif au droit des sociétés commerciales et du groupement d'intérêts économiques ; 209 pages
VI	<b>ROQUES(Pascal)</b> ; Les cahiers du programmeur UML 2 Modéliser une application Web ; Eyrolles ; 2008
VII	<b>TCHANA (Alain)</b> , Le cloud : généralités, Support de cours, 2017

## WEBOGRAPHIE

I	<b>ALEXANDRE BACCO</b> ; Développez votre site web avec le framework Symfony2 (ancienne version); <a href="http://tiny.cc/ifvhmy">tiny.cc/ifvhmy</a> ; consulté en ligne le 01 février 2017
II	<b>BANAT-BERGE(Françoise)</b> ; Gestion et archivage des documents; <a href="http://tiny.cc/6avhmy">tiny.cc/6avhmy</a> ; consulté en ligne le 03 mai 2017
III	<b>BRULEAUX(Anne Marie)</b> ; Préservation et restauration; <a href="http://tiny.cc/7hvhmy">tiny.cc/7hvhmy</a> ; consulté en ligne le 03 mai 2017
IV	<b>CHABIN(Anne Marie)</b> ; Nouveau glossaire d'archivage; consulté en ligne le 03 mai 2017
V	<b>COUTURE (Cynthia)</b> ; Gestion et traitement des archives courantes et intermédiaires; <a href="http://tiny.cc/sivhmy">tiny.cc/sivhmy</a> ; consulté en ligne le 03 mai 2017
VI	<b>DEBANT(Anne)</b> ; Reproduction par microfilmage et numérisation; <a href="http://tiny.cc/nkvhmy">tiny.cc/nkvhmy</a> ; consulté en ligne le 03 mai 2017
VII	<b>DELMAS (Bruno)</b> ; Notions générales d'archivistique; <a href="http://tiny.cc/9kvhmy">tiny.cc/9kvhmy</a> ; consulté en ligne le 03 mai 2017
8 VIII	<b>LAROUSSE(Pierre)</b> ; Dictionnaire Larousse; <a href="http://tiny.cc/pmvhmy">tiny.cc/pmvhmy</a> ; consulté en ligne le 04 juin 2017
IX	<b>LE SERVICE PUBLIC DE DIFFUSION DU DROIT</b> ; Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique(1); <a href="http://tiny.cc/jnvhmy">tiny.cc/jnvhmy</a> ; Consulté en ligne le 07 juillet 2017
X	<b>SENSIOLABS</b> ; Symfony is a set of reusable PHP components; <a href="http://tiny.cc/vnvhmy">tiny.cc/vnvhmy</a> ; consulté en ligne le 02 février 2017
XI	<b>SENSIOLABS</b> ; How to Upload Files; <a href="http://tiny.cc/tovhmy">tiny.cc/tovhmy</a> ; consulté en ligne le 02 février 2017
XII	<b>SENSIOLABS</b> ; Getting Started With FOSUserBundle; <a href="http://tiny.cc/9ovhmy">tiny.cc/9ovhmy</a> ; consulté en ligne le 02 février 2017
XIII	<b>LAROUSSE(Pierre)</b> ; Dictionnaire Larousse; <a href="http://www.larousse.fr/dictionnaires/francais/archivage/5085">http://www.larousse.fr/dictionnaires/francais/archivage/5085</a> ; consulté en ligne le 04 juin 2017
IX	<b>LE SERVICE PUBLIC DE DIFFUSION DU DROIT</b> ; Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature; <a href="http://tiny.cc/urvhmy">tiny.cc/urvhmy</a> électronique(1)

8. A cause de la longueur des url nous avons

X	<b>Sensiolabs</b> , SensioGeneratorBundle, en ligne, <a href="http://tiny.cc/9rvhmy">http://tiny.cc/9rvhmy</a> , consulté le 20 avril 2017
XI	<b>PUGX</b> , PUGXGeneratorBundle ,en ligne, <a href="http://tiny.cc/svhmy">tiny.cc/svhmy</a> ,consulté le 28 Avril 2017
XII	<b>Willdurand</b> , BazingaFakerBundle, en ligne; <a href="http://tiny.cc/8uvhmy">http://tiny.cc/8uvhmy</a> ; consulté le 28 Avril 2017
XIII	<b>FriendsOfSymfony</b> , FOSCommentBundle, <a href="http://tiny.cc/0vvhmy">http://tiny.cc/0vvhmy</a> , en ligne, consulté le 03 mars 2017
XIV	<b>FriendsOfSymfony</b> , FOSUserBundle, <a href="http://tiny.cc/0vvhmy">http://tiny.cc/0vvhmy</a> ,en ligne, consulté le 03 mars 2017

## PRESENTATION DU CENTRE PASTEUR DU CAMEROUN

Le **Centre Pasteur du Cameroun(CPC)** est un Etablissement Public Administratif camerounais doté de l'autonomie financière. Il a été créé en 1959 à Yaoundé ; il dispose depuis 1985 d'une Annexe à Garoua, et d'une antenne à Douala. Il est placé sous la double tutelle des Ministères de la Santé publique et des Finances. Partenaire traditionnel de l'IRD, le Centre Pasteur est membre du Réseau international des Instituts Pasteur dont il partage la mission principale, la lutte contre les maladies infectieuses. Près de 400 personnes viennent quotidiennement au Centre Pasteur pour des analyses biomédicales. Le CPC réalise environ 300000 examens biologiques par an. Ces examens sont réalisés dans les laboratoires :

- Hématologie ;
- Parasitologie ;
- Bactériologie et mycobactériologie-Immunologie ;
- Sérologie ;
- virologie- Biochimie.

Le CPC dispose aussi d'un Laboratoire d'hygiène et de l'environnement qui réalise des analyses microbiologiques et physico chimique des eaux et des aliments, des expertises toxicologiques. Tous ces laboratoires disposent de plateaux techniques uniques au Cameroun, permettant la réalisation d'analyses biologiques de qualité au bénéfice de la population et de la santé publique. Dans sa chaîne de fonctionnement interne, le CPC utilise les logiciels tels que :

- Global Land Ice Measurements from Space (GLIMS) qui permet entre autres de gérer les prélèvements, orienter ces prélèvements vers les laboratoires, collecter les résultats, gérer les factures.
- Optimaint : qui permet aux services supports (Informatique, Bio-informatique) de suivre et effectuer la maintenance de chaque équipements informatiques et automates.
- Sage qui intervient dans les aspects administratifs : finance, comptabilité, paye, achats et ventes

- La suite Microsoft Office 365 qui facilite la communication traitements bureautiques au CPC

