République du Cameroun
****
Paix-Travail-Patrie
****
Ministère de l'Enseignement Supérieur
****
Université de Maroua
****
Ecole Nationale Supérieure
Polytechnique de Maroua

Republic of Cameroon
****
Peace-Work-Fatherland
****
Ministry of Higher Education
****
The University of Maroua
****
The Polytechnic National Advanced
School of Maroua

INFORMATIQUE ET TELECOMMUNICATIONS

CRYPTOGRAPHIE ET SÉCURITÉ INFORMATIQUE

CONCEPTION ET DÉPLOIEMENT D'UN MODULE DE SIGNATURE ÉLECTRONIQUE BASÉ SUR LA PKI

Mémoire présenté et soutenu en vue de l'obtention du Diplôme

D'INGÉNIEUR DE CONCEPTION EN CRYPTOGRAPHIE ET SÉCURITÉ INFORMATIQUE

Par

OUMAR DJIMÉ RATOU

Matricule : 17Y402P

Sous la Direction de :

Dr. KALADZAVI GUIDEDI

Chargé de Cours

Devant le jury composé de :

Président : *M. LAOUKOURA Charles*
Rapporteur : *M. LAOUKOURA Charles*
Examinateur : *M. LAOUKOURA Charles*

ANNÉE ACADÉMIQUE: **2018/2019**

Dédicaces

Remerciement

Table des matières

Listes des abréviations

Résumé

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Abstract

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Keyswords ou mot clé

Liste des tableaux

Table des figures

Introduction

Première partie

Présentation générale

Chapitre 1

Contexte et problématique

Introduction

DANS ce chapitre de la première partie, nous présentons l'entreprise où nous avons effectué notre stage académique à savoir ITS. Nous parlerons ensuite du contexte relatif à notre sujet de stage de fin d'étude, nous terminerons par une mise en évidence de la problématique lié à ce contexte et les objectifs à atteindre.

1.1 Présentation de l'entreprise

1.1.1 Historique

ITS est une entreprise spécialisée dans la protection des systèmes d'informations, la sécurité informatique et la cryptologie de droit camerounais dont le siège générale se trouve à Yaoundé-Cameroun BP : 8570, plus précisément à Byem-Assi dans le 6^{me} arrondissement du département de MFOUNDI. Elle commence ces services depuis 2008.

1.1.2 Organisation générale

1.1.3 Missions

ITS est une entreprise résolument tournée vers l'innovation et en constante croissance. La mission d'ITS est de fournir à toute les entreprises et organismes publics, quelle que soit leur taille, les solutions des outils cryptographiques, de sécurité réseaux et de sécurités de systèmes d'informations le plus performant du marché. ITS fondé en 2008, est une entreprise leader dans le domaine de cryptographie et de sécurité des systèmes d'informations au Cameroun. Les solutions apportées par ITS permettent à leurs clients d'avoir l'assurance qu'une faille de sécurité ne menacera jamais leurs activités. Ils peuvent donc consacrer totalement à leur croissance, car ces solutions les protègent efficacement contre les risques et les menaces informatiques. D'ailleurs sa réputation tient à la qualité des solutions de sécurités qu'elle met en place depuis sa création. Celles-ci intègrent les fonctionnalités essentiels suivantes :

- prévention d'intrusion (IDS),
- par-feu,
- protection antivirale et antispware,
- filtrage antispam et de contenu,
- PKI (Public Key Infrastructure),
- mobilité sécurité VPN,
- outils cryptographiques,
- etc.

Et enfin elle édifie les personnels des entreprises à travers de conférences, séminaires et webinaires et forme les intéressés dans plusieurs domaine de la sécurité informatique en vue de l'obtention de certificat à la fin de chaque formation.

1.1.4 Services et Produits

Entreprise ITS renferme plusieurs services, E-services et une centre de formations :

Sévices

Les services sont :

- **Sécurité des SI :** Aujourd'hui l'implémentation des technologies de l'information et de la communication engendre les problèmes de types nouveaux de sécurité des informations sensibles,des infrastructures et organisations mises en place. Ainsi le contrôle et la gestion du risque informationnel dans ces nouveaux systèmes deviennent indispensables pour le bon fonctionnement et même l'existence de ces derniers.
- **Investigation Numériques :**La cybercriminalité gagne du terrain avec la globalisation des systèmes d'information et l'intensification de leur utilisation dans tous les domaines d'activités de l'homme. La coopération internationale ne promet pas de résultats intéressants en même temps que les cybercriminels exploitent de mieux en mieux les technologies d'attaques disponibles, et ceci dans des conditions de partage d'expériences très bonnes. La police et les services de sécurité traînent le pas même si la législation permettant de combattre le fléau prend corps. La loi ne peut être efficace que si la preuve numérique du crime commis est à la disposition de la justice.
- **Audit des SI :**L'utilisation des systèmes d'information de plus en plus complexes et leur implémentation dans le contrôle et la gestion des processus sensibles imposent une normalisation visant la conformité de tous les systèmes d'information selon l'activité et le métier dans le but de mieux maitriser le risque qu'engendre le système d'information dans

le fonctionnement de toute organisation. Ainsi l'audit des systèmes d'information comme activité visant a mesurer le niveau de conformité d'un système d'information par rapport a des règles bien définies et a examiner le niveau de dérive du système par rapport a ces standards aide a anticiper sur les problèmes et a proposer les solutions pour y remédier avant même l'occurrence d'incidents.

- **Gouvernance des SI :**Toute activité nécessite un système de gouvernance solide et efficace pour s'assurer de la pérennité de cette dernière, ainsi que de l'atteinte des objectifs fixe au départ. Le système d'information ne s'aurait faire exception à cette règle, au contraire nécessite plus d'attention dans ce sens car complexe et indispensable pour toute entreprise. Les investissements fais pour son système d'information doivent se justifier non pas par un besoin simple, mais au moyen d'une étude préalable présentant le gain retour sur cet investissement par la création et l'exploitation des services lies à l'investissement en question.

E-Services

Dans les e-services on a plusieurs catégories :

1. **Web conférences :** rencontre internationale de Yaoundé sur la gestion du secret, l'usage de la cryptographie (Science du secret) dans la protection de l'information stratégique, la maîtrise des méthodes, moyens et systèmes de protection de l'information.
2. **Web séminaires**
   - **webinaire**[1] **Protection d'informations stratégiques :** Cette formation a pour objectif, la maîtrise des techniques de sécurisation et protection des informations stratégiques, ainsi que l'étude des mécanisme de protection de donnés sensibles.
   - **webinaire : Audit informatique :** Le but de la formation est la maîtrise des notions et techniques d'audit des systèmes d'information, ainsi que l'étude des cas selon une démarche spécifique.
3. Web consultations
4. E-Catalogue

Formations

Le centre de formation ITS est un centre de formation de référence spécialise dans les modules de formation suivants :

- sécurité des système d'information ;

[1]Webinaire est un mot-valise associant les mots web et séminaire, créé pour désigner toutes les formes de réunions interactives de type séminaire faites via internet généralement dans un but de travail collaboratif ou d'enseignement à distance

- investigations numériques ;
- audit des systèmes d'information ;
- gouvernance des systèmes d'information ;
- développement informatique ;
- infographie.

Les formations ont un cycle de douze mois soit neuf mois de cours et trois mois de pratique en entreprise. Le centre de formation CF-ITS est agrée par le MINEFOPE(Ministère de l'Emploi et de la Formation Professionnelle) et donc délivre les certificats de fin de formation conformément à la réglementation en vigueur. En marge des formation dans les salles.

Le centre donne l'accès gratuit et illimité aux forums et discussions via le portail web linkedin(www.linkedin.com) avec un nombre illimité d'experts internationaux du domaine de la cybercriminalité, cybersécurité, et investigation numériques, gouvernance et audit des systèmes d'information.

Certifications

ITS offre également des certifications suivants :

1. Certification Professionnelle Nationale (MINEFOP)
    - Sécurité des systèmes d'Informations
    - Investigations numériques
    - Audit des systèmes d'information
    - Gouvernance des systèmes d'information
2. Certification Professionnelle Internationale (ISACA)
    - CISM - Certified Information Security Manager
    - CISA - certified Information Systems Auditor
    - CRISC - Certified in Risk and Information Systems Control
    - CGEIT-Certified in Governance of Enterprise IT
3. Certification Professionnelle Internationale (CISCO)

Produits

L'entreprise a mis à la disposition de tout le monde des logiciels gratuit, on peut citer entre autre les logiciels suivants :

- Utilitaire de désinstallation d'antivirus **AVAST**,

- Logiciel de calcul de l'empreinte numérique des fichiers,
- Calcul du hash code des fichier par **MD5**,
- Logiciel d'**EBIOS**,
- Logiciel de stéganographie,
- **Ntop** - Logiciel de **monitoring** du réseau.

Et des logiciels payants :

- Logiciel de récupération de mots de passe,
- etc.

1.1.5 Cadre de stage

On a effectué notre stage au sein de la direction général de l'entreprise, elle se trouve dans le quartier **Biyem-Assi** dans la ville de Yaoundé, département de MFOUNDI plus précisément situé en plein cœur du 6e arrondissement. Leur direction se trouve dans l'**Avenue Biyem-Assi** à côté de **Pharmacie Les Béatitudes**.

Situation géographique

La figure ci-dessous présente l'emplacement de notre lieu de stage réalisé grâce au service du géant Google **Google Map**.

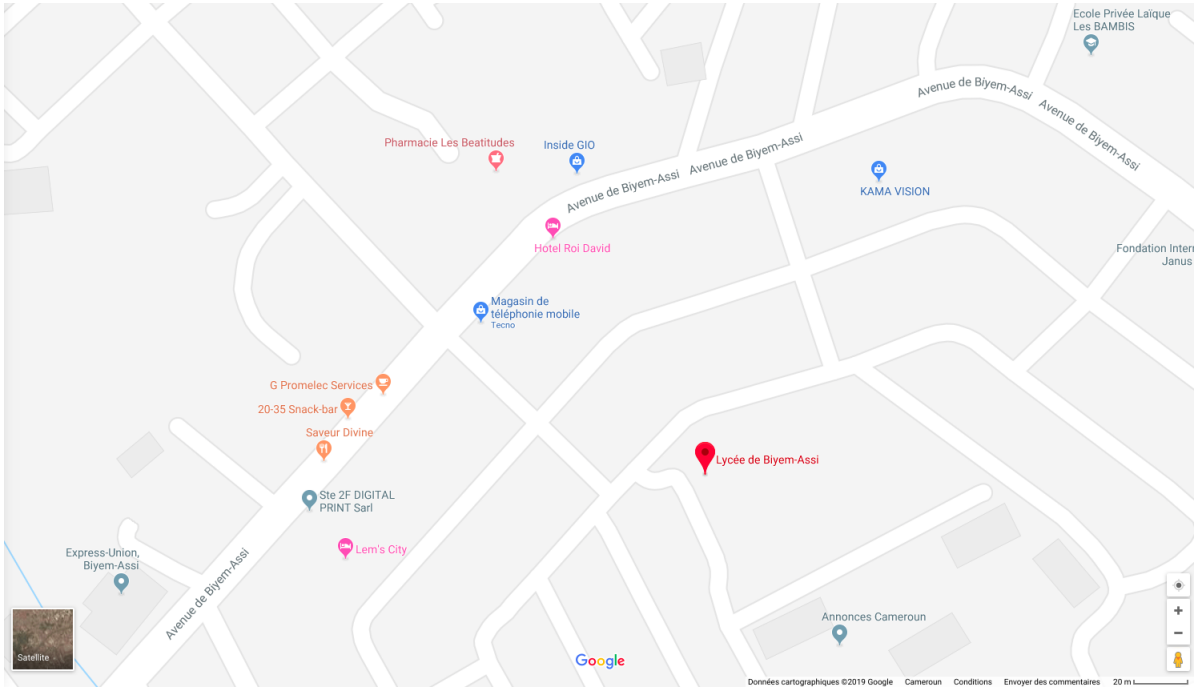

FIGURE 1.1 – Situation géographique du lieu de stage

1.2 Contexte

La création des signatures électroniques basé sur les infrastructures à clé publiques que sa soit avec OpenSSL ou d'autres se font soit en console, soit d'utiliser des outils propriétaires tels que :

- Word pour Microsoft,
- Adobe Reader de l'entreprise Adobe,
- DocuSign,
- Eversign,
- Yousign,

soit d'aller chez une Autorité de Certification (AC) pour générer un certificat, qui sont complexes et coûteux pour les utilisateurs et surtout à ceux qui débutent en développement des applications et en sécurité informatique. Et encore malheureusement ils sont déjà intégrés dans leurs applications complètes, donc pas des moyens de les réutiliser dans d'autres logiciels comme des modules.

Par ailleurs d'autres ne sont pas dans les systèmes d'exploitation libre(open source) comme Linux, par exemple **Word** de Microsoft et **Adobe Reader** ne fonctionnent pas sous Linux.

1.3 Problématique

Les problèmes qui surviennent souvent dans les entreprises en particulier et chez les développeurs en général c'est la disposition des programmes modulaires pour intégrer facilement dans leurs plates-formes en fin de gagner en temps et en l'argent (surtout pour les entreprises). Ces nécessités nous amènent à nous poser les questions suivantes :

- Comment peut-on rendre cette difficulté de signer un document de manière transparente ?
- Comment faciliter le développement d'un outil informatique au sein de l'entreprise ?
- Comment développer un module multi-plateforme ?

1.4 Objectifs

1.4.1 Objectif général

L'objectif principal de notre projet est d'offrir à l'entreprise et toute personne désirant signer un document électroniquement, un outil de signature électronique modulable.

1.4.2 Objectif spécifique

De façon spécifique, il sera question pour moi de gérer les problèmes spécifiques liés aux :

- Création d'une signature des documents numériques (texte, son, vidéo, PDF, etc.) en se basant sur les infrastructures à clé publique ou PKI,
- automatisation de la création des signatures numériques,
- vérification de la signature de document numérique,
- prouver l'authenticité d'un signataire,
- faciliter à l'entreprise lors d'un besoin d'un module de signature électronique,
- génération des clés et chiffrement/déchiffrement des données,
- rendre la vie facile au développeur qui ne maîtrise pas forcément la notion de cryptographie qui se cache derrière la signature numérique, d'intégrer ce module dans son plate-forme.

Ainsi les utilisateur avertis pourront juste l'importer dans leurs programmes et l'utilisé facilement. Tout ce qu'un utilisateur doit connaître c'est le nom de la méthode qu'il veut appeler avec sa signature (les paramètres de la méthode) et la méthode retournera le résultat voulu. Il y'aura une commande d'aide si l'utilisateur ne connais pas le nom de la méthode avec sa signature(paramètre) et une manuelle bien documenté avec des exemples d'utilisations.

1.5 Méthodologie

Pour atteindre ces objectifs, nous proposons à l'entreprise la conception et le déploiement d'un module de signature électronique basé sur l'infrastructure à clé publique (PKI). Nous allons suivre le cheminement de la conception dont les grandes étapes sont suivantes :

1. L'analyse des besoins du client qui débouchera sur l'élaboration d'un cahier de charges ;
2. La conception du système qui débouchera sur la modélisation des différentes vues du système ;
3. L'implémentation logicielle qui est le codage proprement dit des différents éléments du système ;
4. Et enfin nous procéderons au déploiement, aux tests et validation.

Conclusion

Dans ce chapitre de la première partie nous avons présenté le contexte et la problématique liés à notre thème et les services et produits que proposent ITS. En énumérant les problèmes que rencontre l'entreprise, les développeurs et les usagés lors de la signature électronique des documents numérique que nous proposons de résoudre par la mise en place de la conception et déploiement d'un module de signature électronique en se basant sur la infrastructure à clé publique. Dans le chapitre suivant, nous présenterons les généralités liés à la signature électronique en particulier et la cryptographie en générale.

Chapitre 2

Généralités sur la signature électronique et PKI

Introduction

2.1 Généralités sur la signature électronique

2.1.1 Signature électronique

Définitions

Rôle de signature électronique

2.2 Cryptographie

2.2.1 Cryptographie symétrique

2.2.2 Cryptographie asymétrique

2.3 Infrastructure à clé publique

Conclusion

Deuxième partie

Conception, analyse et implémentation

Chapitre 3

Analyse, Conception et déploiement du module

Introduction

Une fois que la présentation des concepts liée à notre projet est faite, nous allons effectuer l'analyse et la conception de notre module de signature électronique. Pour cela, nous effectuerons premièrement le choix de cycle de vie de développement d'un logiciel qui nous convient, deuxièmement nous procéderons à l'analyse de besoins, ensuite nous ferons la conception proprement dite et enfin nous terminerons par l'implémentation du système.

3.1 Choix du cycle de développement

Le cycle de vie d'un logiciel indique les étapes par lesquelles doit passer un logiciel de sa conception jusqu'à sa mort. Ce cycle de vie permet de détecter les erreurs tout au long du processus de réalisation et ainsi les corriger pour produire un logiciel de qualité, maîtriser les délais de sa réalisation et les coûts associés. Le cycle de vie d'un logiciel comprend généralement les étapes suivantes :

1. **Pré-étude :** Cette étape permet de définir les objectifs du projet de définir le domaine d'activité. Les questions poser sont :**Quoi ?, Combien ? et Quoi ?**

   En entrée, on a les besoins et en sortie on a un cahier de charges.

2. **Analyse :** Cette consiste à recueillir les informations et formaliser les besoins du client, de définir les contraintes et d'estimer la faisabilité de ce besoins. La question à poser est : **que fait le système ?**

   En entré, on a le cahier de charge et en sortie on a le dossier d'analyse.

3. **Conception :** Cette étape permet d'élaborer la structure générale du système et de définir chaque sous-ensemble de logiciel à produire. La question à poser est : **comment faire ce qu'il est demandé de faire ?**

En entré, on a le dossier d'analyse et en sortie on a un dossier de conception.

4. **Codage :** Cette étape consiste à coder ou à programmer les fonctionnalités définis dans la phase de conception.

   En entré, on a le dossier de conception en sortie on a des programmes.

5. **Tests :** Cette étape permet de tester le logiciel conformément aux spécifications(fonctionnelle ou non fonctionnelle). Il existe quatre types de tests à savoir : **le test unitaire, le test d'intégration, le test fonctionnel et le test de validation.**

6. **Réception :** Cette étape permet au client de vérifier la conformité de logiciel avec les spécifications initiales.

   *En entré on a un logiciel plus un cahier de charge et en sortie on a un procès verbal de réception****(acception ou refus du livrable)****.*

7. **Maintenance :** Cette étape permet de prendre en charge les actions collectives du système**(Maintenance collective et évolutive).**

   En entré on a un logiciel et en sortie on a un logiciel modifié.

Nous avons vu quelles sont les étapes clés dans le cycle de vie d'une application. Afin d'obtenir un résultat optimal, il est conseillé de suivre cette démarche qui peut subir des améliorations[**?**]. Il existe plusieurs modèles de cycle de vie à savoir : le cycle en cascade, le cycle en V, le cycle en spirale, le cycle semi-itératif mais dans notre cas on a décider de suivre le modèle du cycle en V.

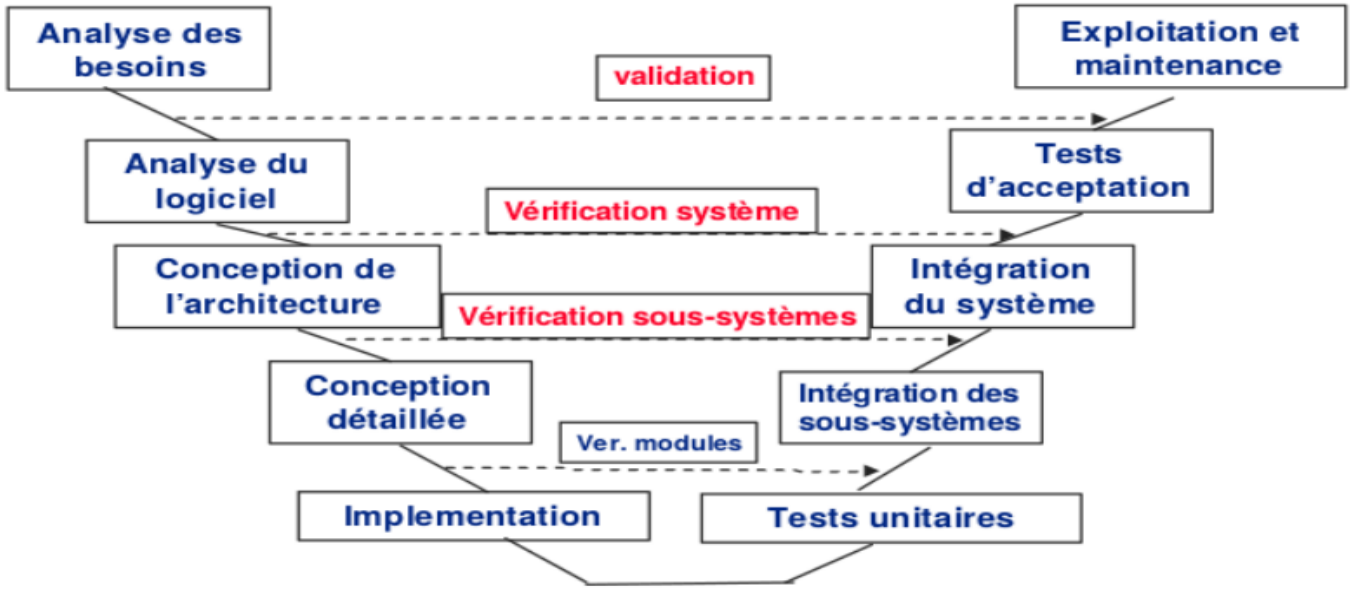

FIGURE 3.1 – Modèle de cycle en V

Pourquoi cycle en V ?

Il est introduit en **1997**. La version actuelle est désignée de **V-Modell XT**(depuis février 2005). Cette méthode consiste en un modèle pour la planification et le développement de logiciel[**?**]. Le

modèle V répond à quatre requête importantes de développement : **Who ? What ? When ? How ?**
L'on peut poser la question comme suit : **Who has to do what, when, and how whithin a project ? Qui doit faire quoi, quand et comment dans un projet ?** Cette question est capital lors de la construction d'un logiciel.
Par ailleurs, dans le modèle V, le fond réalise l'implémentation. La branche gauche définit les différentes spécifications. La branche droite crée des corrélations avec la partie gauche à savoir la validation du système, la vérification système et du logiciel.
L'accent est mis sur la réduction des erreurs. La branche droite permet en général la détection rapide des erreurs et des anomalies présents dans la partie gauche et entreprend des mesures adéquates pour les corriger. Et en plus, la finalité de cycle de vie en V consiste à parvenir sans incident à livrer un logiciel totalement conforme au cahier des charges[**?**]. Voila pourquoi nous avons choisi le modèle V.

3.2 Orientation et faisabilité

Le projet intitulé « Conception et déploiement d'un module de signature numérique basé sur l'architecture à clé publique »est né du fait que l'entreprise ITS à constater qu'il n'y a pas un module de signature électronique disponible pour les développeurs pour intégrer dans leurs plate-formes en général et un système de complet de signature électronique libre et transparent en particulier.
Par ailleurs, bien qu'ils existent des tels systèmes tels que Word de Microsoft et Adobe Reader mais ne sont pas dans les systèmes d'exploitation libre(open source) comme Linux.
Les problèmes qui surviennent souvent dans les entreprises en particulier et chez les développeurs en général c'est la disposition des programmes modulaires pour intégrer facilement dans leurs plates-formes en fin de gagner en temps et en l'argent (surtout pour les entreprises).
L'environnement dans lequel nous nous trouvons est favorable au projet puisqu'un tel système existe certes mais sous une licence payante et non modulable. Sa mise en œuvre sera une innovation importante dans l'évolution numérique au sein de l'entreprise et dans le monde de open source.
L'utilisation du système bénéficiera à ITS de :

- Signer désormais ces documents numériques,
- Utiliser le module dans un projet de même thématique facilement,
- permet d'avoir son propre outil de signature électronique.

Ce projet d'inscrit donc largement dans le cadre de la sécurité de système d'information qui est aujourd'hui très capital tant pour les entreprises que les utilisateurs.

3.3 Analyse de besoins

Dans cette section, nous allons recueillir les besoins du demandeur (le client) et l'ensemble des contraintes liés au système à mettre sur pied.

3.3.1 Cahier de charge

Le cahier de charge a pour but de présenter notre projet su la signature électronique basé sur l'architecture à clé publique des documents numériques de l'entreprise ITS et autres tel que spécifié dans la section précédente.

Besoins fonctionnels

Il est question ici de présenter toutes les fonctionnalités du système. Ce sont les besoins spécifiant un comportement d'entré/sortie du système. Le système doit permettre à :

1. l'Administrateur de :
    - gérer les comptes (supprimer, modifier, bloquer etc),
    - générer une paire de clé(publique et privée),
    - signer un document numérique à l'aide de la clé privée,
    - générer un certificat (auto-signé, puisque le signé est payant),
    - vérifier la signature d'un document numérique à l'aide de la clé publique,
    - chiffrer/déchiffrer un document,
    - générer un Hash du document numérique.

    Il faut noter que l'administrateur ne pourra effectuer ces fonctionnalités que s'il est authentifier avec son compte administrateur, question de sécurité.

2. l'Utilisateur de :
    - générer une paire de clé(publique et privée),
    - signer un document numérique à l'aide de la clé privée,
    - générer un certificat (auto-signé, puisque le signé est payant),
    - vérifier la signature d'un document numérique à l'aide de la clé publique,
    - chiffrer/déchiffrer un document,
    - générer un Hash du document numérique.

3. au système externe de :
    - générer une paire de clé(publique et privée),
    - signer un document numérique à l'aide de la clé privée,

- générer un certificat (auto-signé, puisque le signé est payant),
- vérifier la signature d'un document numérique à l'aide de la clé publique,
- chiffrer/déchiffrer un document,
- générer un Hash du document numérique.

Besoins non fonctionnels

A part les besoins fondamentaux, notre système doit répondre aux critère suivants :

- la rapidité de traitement : En effet, vu le nombre important des transactions quotidiennes, il est impérativement nécessaire que la durée d'exécution des traitements s'approche le plus possible du temps réel ;
- la performance : Un logiciel doit être avant tout performant c'est-à-dire à travers ses fonctionnalités, répond à toutes les exigences des usagers d'une manière optimale ;
- La convivialité : Le futur logiciel doit être facile à utiliser. En effet, les interfaces utilisateurs doivent être conviviales c'est-à-dire simples, ergonomiques et adaptées à l'utilisateur.

Elle devra aussi être capable de :

- tourner en réseaux pour qu'il soit accessible de tous,
- être compatible avec n'importe quel système d'exploitation, smartphone, tablette et OS.

Il faut aussi souligner que l'application devra être hautement sécurisé car les informations ne devront pas être accessible de tous, sauf pour les légitimes.

3.4 Budgétisation

Ressources	Noms	Quantité	Prix unitaire	Total
Tétraèdre	4	6	4	4+4-6=2
Cube	8	12	6	8+6-12=2

3.5 Conception architecturale

Nous élaborons les spécifications de notre architecture générale de notre système. Nous optons pour une architecture client serveur centralisée. L'environnement client/serveur désigne un mode de communication organisé par l'intermédiaire d'un réseau et d'un interface Web entre plusieurs ordinateurs . « cela signifie que des machines clientes (machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en terme de capacités d'entrées-sorties , qui leur fournit des services. Lesquels services sont exploités par des programmes ,appelés programmes clients, s'exécutant sur les machines clientes. »

Puisqu'il existe plusieurs environnements client/serveur(Architecture "**Peer to Peer**",Architecture à 2 niveaux,Architecture à 3 niveaux, etc), plus précisément nous optons pour une architecture client/serveur Peer to Peer. Le réseau est dit pair à pair (peer-to-peer en anglais, ou P2P), lorsque chaque terminal connecté au réseau est susceptible de jouer tour à tour le rôle de client et celui de serveur.

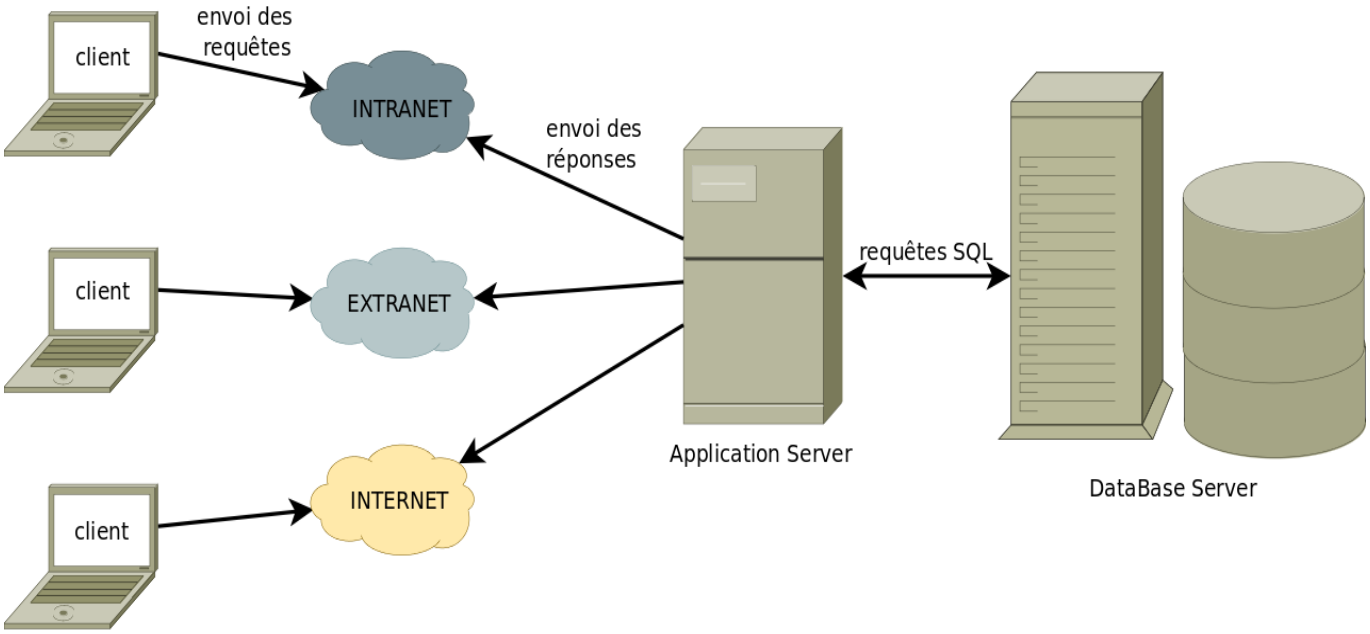

FIGURE 3.2 – Architecture Client Serveur

3.6 Conception détaillée

Pour réaliser la conception détaillée de notre système nous utiliserons le langage de modélisation UML (Unified Modeling Language).

3.6.1 Présentation de langage UML

L'UML (pour Unified Modeling Language, ou "langage de modélisation unifié" en français) est un langage permettant de modéliser nos classes et leurs interactions. Autrement c'est un ensemble de notations graphiques s'appuyant sur des diagrammes et permettant de spécifier, visualiser et de documenter les systèmes logiciels orientés-objet. UML utilise des diagrammes pour modéliser un système. Il ne s'agit pas d'une simple notation graphique car les concepts

transmis par un diagramme ont une sémantique[?].
En ce qui concerne la structure du formalisme UML, il peut être vu comme nous montre la figure suivante :

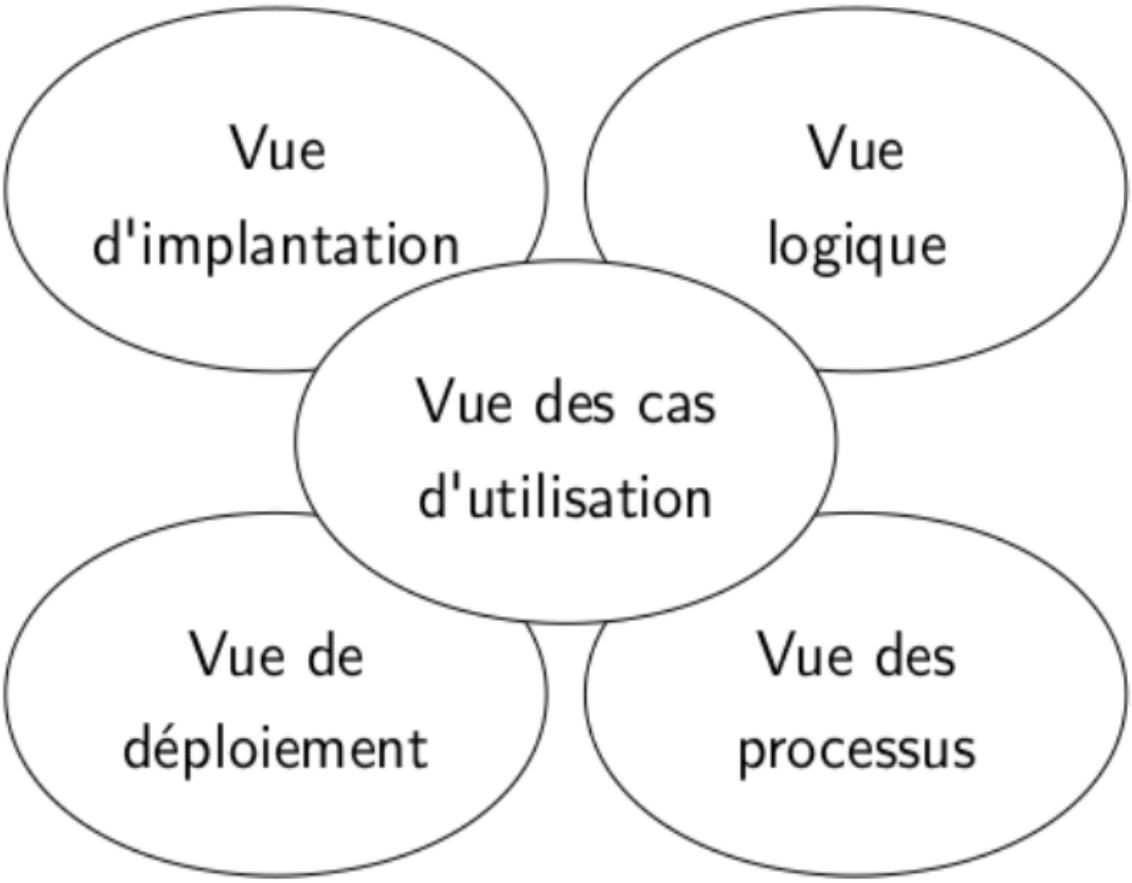

FIGURE 3.3 – différentes vues du formalisme UML

A chaque vue est associée certains diagramme :

- **Vue de cas d'utilisation[?] :** S'applique à l'ensemble des cas d'utilisation qui décrivent ensemble le comportement d'un système donné vu par ses acteurs. Cette vue indique les forces internes et externes qui forment l'architecture du système. Elle définit les besoins des clients du système et centre la définition de l'architecture du système sur la réalisation de ces besoins ; elle conduit à la définition d'un modèle d'architecture pertinent et cohérent en se basant sur les scénarios décrits dans les cas d'utilisation.

  Elle motive les choix, permet d'identifier les interfaces critiques et force à se concentrer sur les problèmes importants.

- **Vue logique :** a pour but d'identifier les éléments du domaine, les relations et interactions entre ces éléments. Cette vue organise les éléments du domaine en « catégories ». Deux diagrammes peuvent être utilisés pour cette vue : diagramme de classes et diagramme des objets.

- **Vue des processus :** Démontre la décomposition système en processus et actions, les interactions entres les processus, la synchronisation et la communication des activités parallèles. Elle s'appuie sur plusieurs diagrammes : diagramme de séquence, diagramme d'activité, diagramme de collaboration etc.
- **Vue de déploiement :** décrit les ressources matérielles et la répartition des parties du logiciel sur ces éléments. Il contient un diagramme : le diagramme de déploiement.
- **Vue d'implémentation :** Décrit l'ensemble des algorithmes utilisés et le code source[**?**].

3.6.2 Modélisation avec le langage UML

Pour modéliser notre système avec le langage UML, nous allons utiliser les outils suivants :

1. Astah-pro, version d'évaluation,
2. Umbrello,
3. GIMP 2.10.

Diagramme de cas d'utilisation

Le diagramme des cas d'utilisation est une notation très simple et compréhensible par tous et qui permet de structurer les besoins (cahier des charges) et le reste du développement. Un diagramme de cas d'utilisation décrit les acteurs[1], les cas d'utilisation[2] et le système. Un modèle de cas utilisation peut être formé de plusieurs diagrammes de cas d'utilisation, de descriptions textuelles, de diagrammes de séquences. Un cas d'utilisation CU) décrit une manière d'utiliser le système en une suite d'interactions entre un acteur et le système.

1. **Diagramme de cas d'utilisation général :**

[1]Un acteur est un utilisateur, humain ou non, du système qui est doté d'un nom qui correspond à son rôle.
[2]Un cas d'utilisation est une manière spécifique d'utiliser le système.

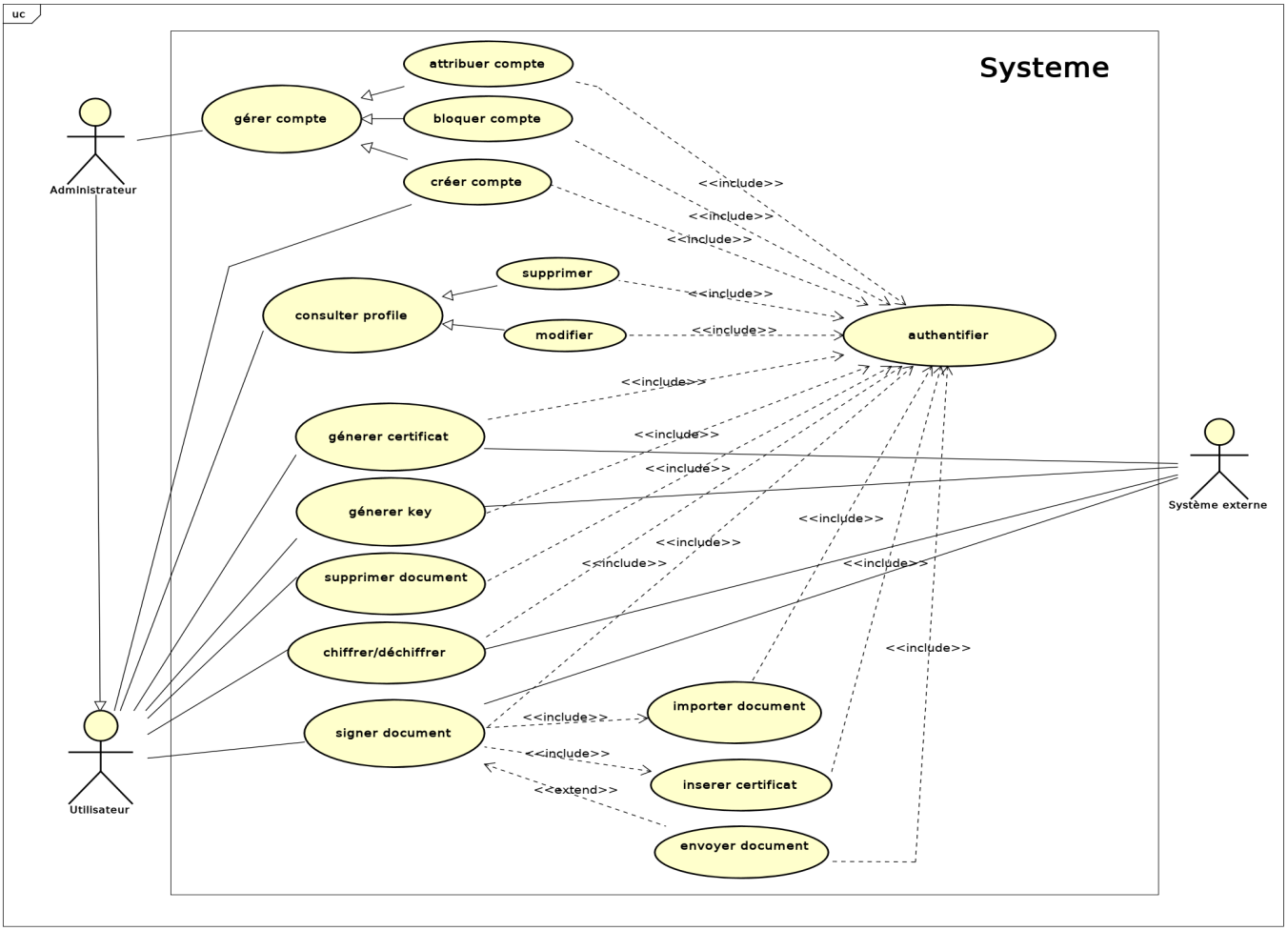

FIGURE 3.4 – Diagramme de cas d'utilisation général

2. **Diagramme de cas d'utilisation de l'administrateur :**

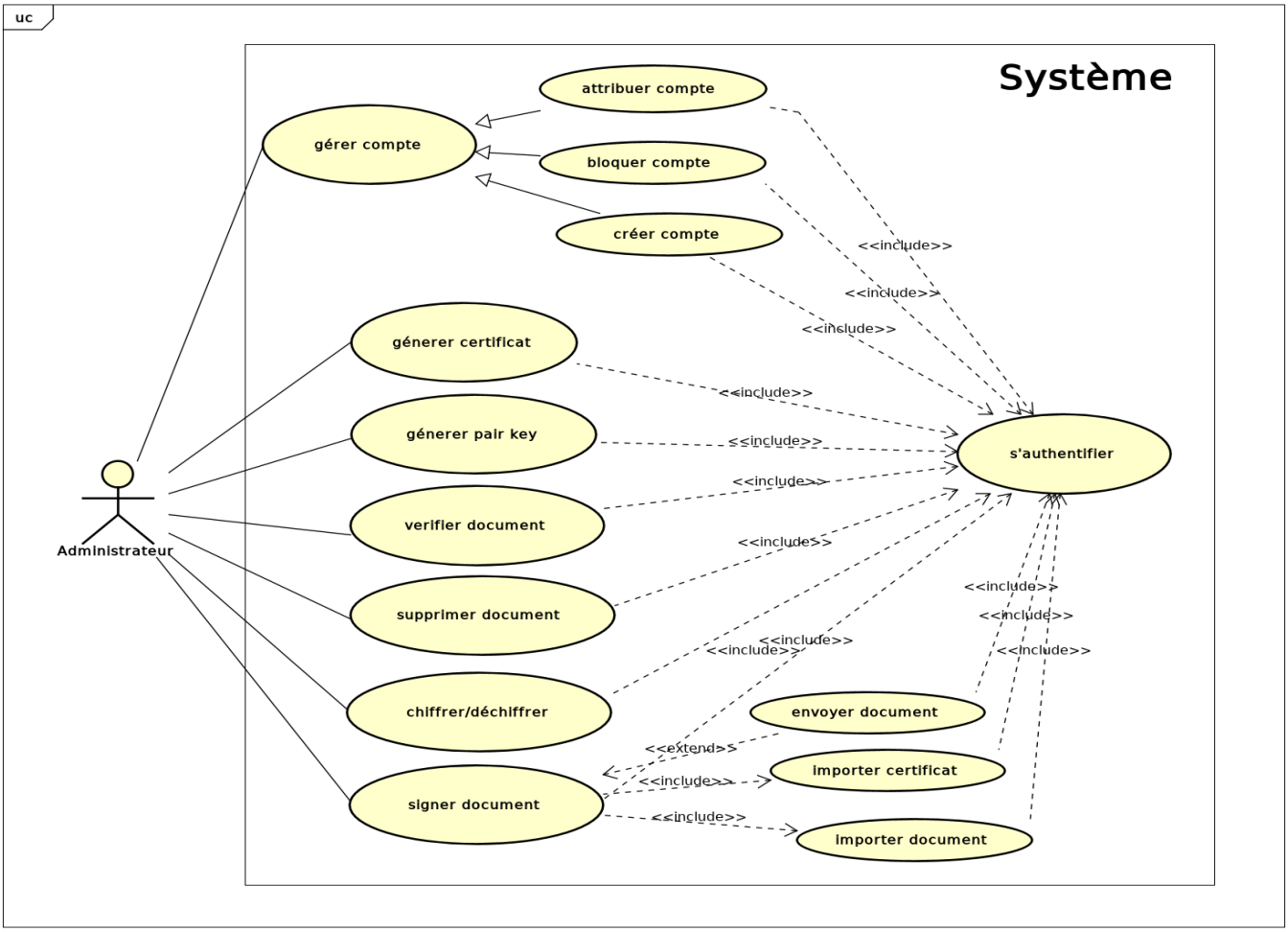

FIGURE 3.5 – Diagramme de cas d'utilisation d'administrateur

3. **Diagramme de cas d'utilisation de l'utilisateur :**

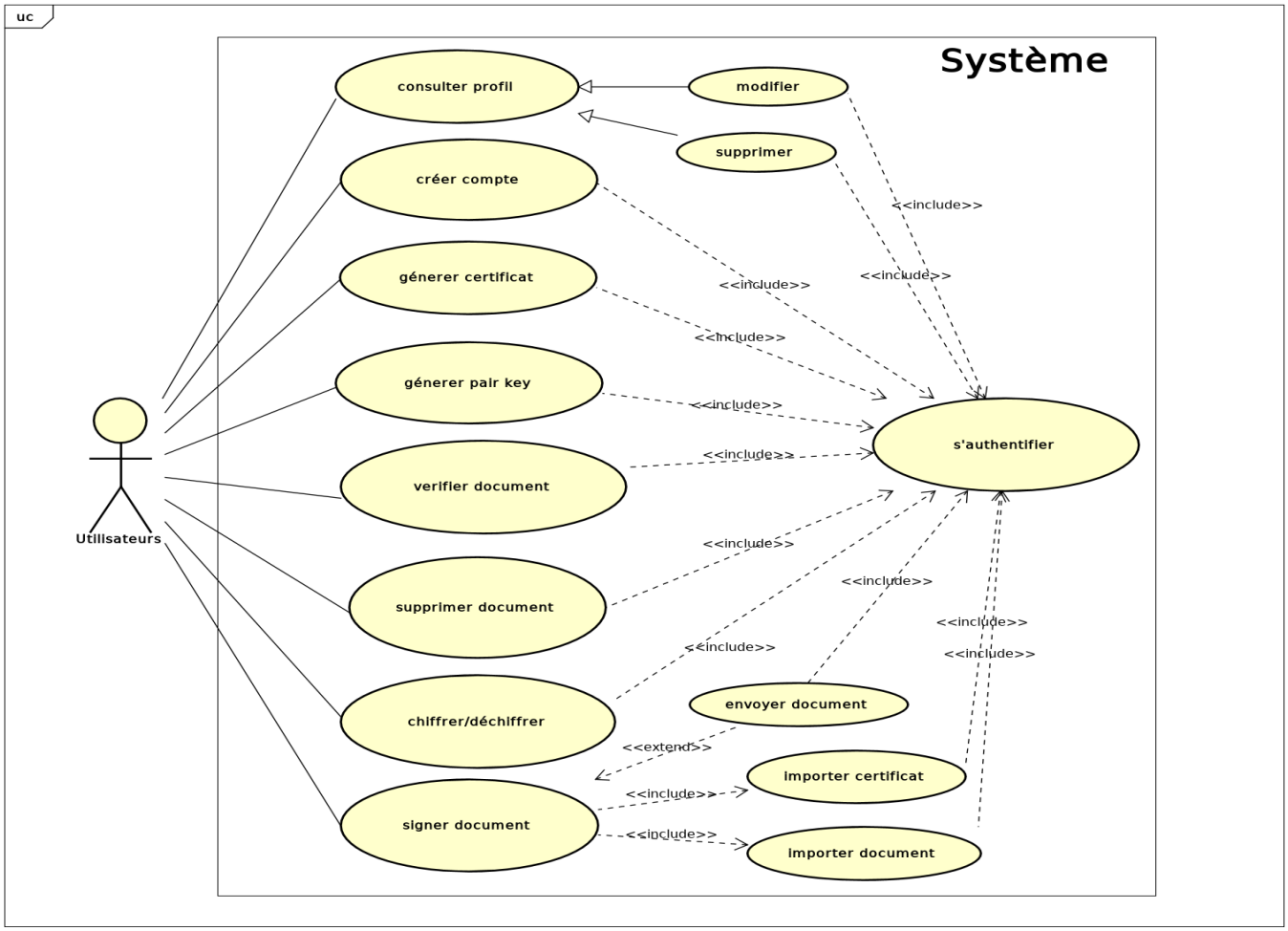

FIGURE 3.6 – Diagramme de cas d'utilisation d'utilisateur

4. **Diagramme de cas d'utilisation de système externe :**

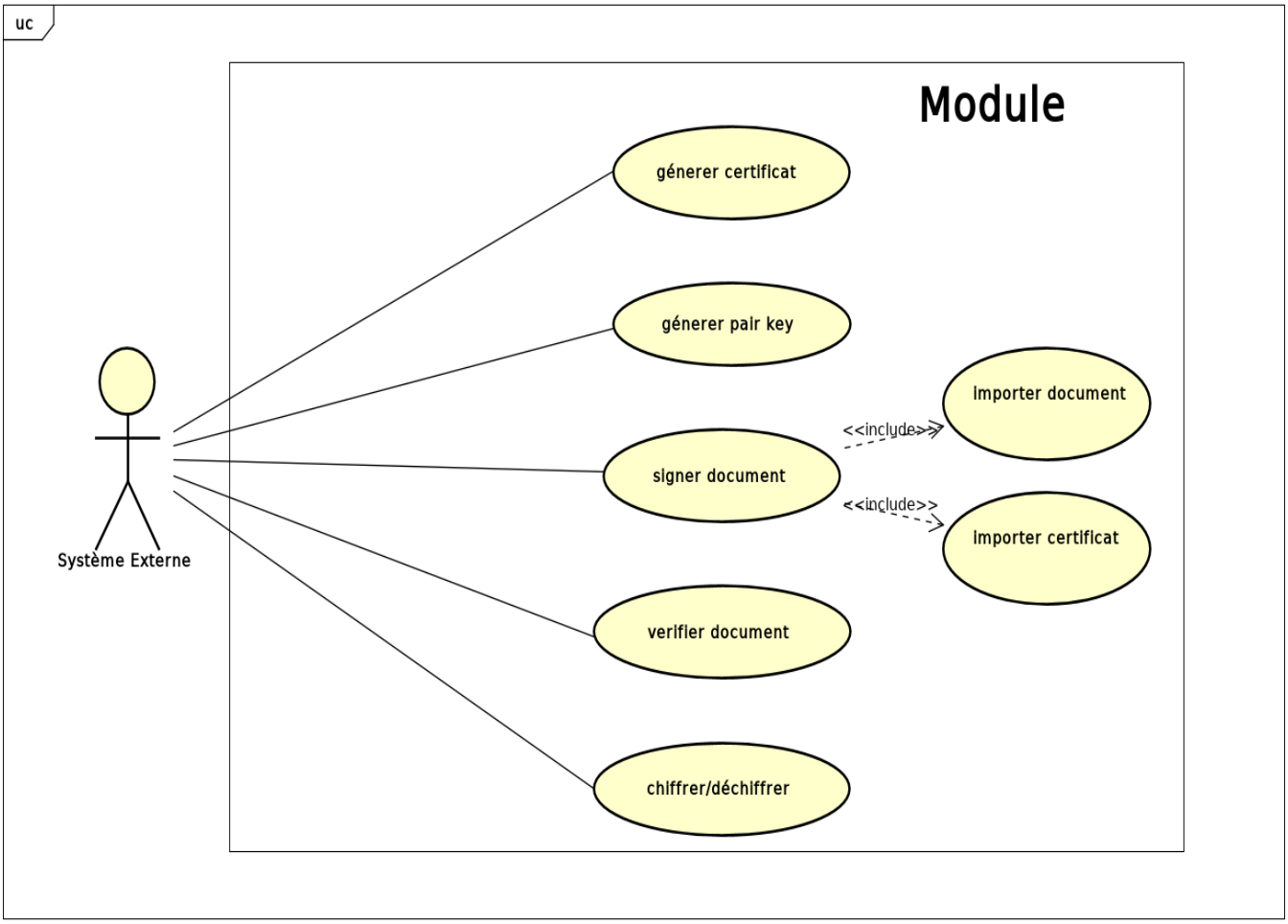

FIGURE 3.7 – Diagramme de cas d'utilisation de système externe

Description textuelle

1. Description textuelle de cas d'utilisation : **S'authentifier**

TABLE 3.1 – Description contextuelle de cas d'utilisation s'authentifier

Titre	S'authentifier
Résumé	Ce cas d'utilisation permet d'accéder au tableau de bord de l'utilisateur
Acteur	Administrateur, utilisateur
Pré-condition	l'application doit être lancer(page d'accueil)
Scenario nominal	1) l'utilisateur fait une demande l'accès au système en cliquant sur le bouton connexion, 2) le système lui renvoi le formulaire de connexion 3) l'utilisateur introduit son username et password 4) le système vérifie que sont username et password corrects 5) le système ouvre une session de l'utilisateur
Enchaînement Alternatif	le username et le password sont corrects., l'enchaînement commence au point 3 du scénario nominal. le message affiche un message d'erreur, aller au point 2.
Enchaînement d'Erreur	E1 : Si l'étape 2 de scenario nominal n'est pas vérifié un message d'erreur sera affiché.
Post condition	ouverture d'une session, accès au compte

2. Description textuelle de cas d'utilisation : **Générer certificat**

TABLE 3.2 – Description contextuelle de cas d'utilisation générer certificat

Titre	Générer Certificat
Résumé	Ce cas d'utilisation permet de générer des certificats aux utilisateurs
Acteur	Autorité de certification Administrateur, Système externe
Pré-condition	l'application doit être lancer (page d'accueil)
Scenario nominal	1) un AC peut générer un certificat en cliquant sur le bouton genererCertifcat, 2) le système lui renvoi le formulaire à remplir 3) on introduit la clé publique de l'utilisateur 4) on renseigne le nom et le prénom de l'utilisateur 5) la date de validité (début et fin) 6) numéro de version 7) numéro de série.
Enchaînement Alternatif	la clé publique n'est pas corrects. l'enchaînement commence au point 2 du scénario nominal.
Enchaînement d'Erreur	E1 : Si l'étape 2 de scenario nominal n'est pas vérifié un message d'erreur sera affiché.
Post condition	création de certificat avec succès.

3. Description textuelle de cas d'utilisation : **Générer Paire de Clé**

TABLE 3.3 – Description contextuelle de cas d'utilisation générer paire de clé

Titre	Générer Paire de clé
Résumé	Ce cas d'utilisation permet de générer des paires de clé aux utilisateurs
Acteur	Autorité de certification, Administrateur, Système externe, Utilisateur
Pré-condition	l'application doit être lancer (page d'accueil) et l'utilisateur est authentifié
Scenario nominal	1) un utilisateur peut générer une paire en cliquant sur le bouton genererPaireKey, 2) le système lui renvoi le formulaire à remplir 3) il introduit le cryptosystème à utiliser (ex. RSA) 4) ensuite il introduit la taille de clé (ex.4096) 5) il valide en cliquant sur le bouton générer
Enchaînement Alternatif	l'algorithme ou la taille de clé est incorrect. l'enchaînement commence au point 2 du scénario nominal.
Enchaînement d'Erreur	E1 : Si l'étape 3 de scenario nominal est incorrect, un message d'erreur sera affiché. Si l'étape 4 de scenario nominal est incorrect, un message d'erreur sera affiché.
Post condition	génération de paire de clé avec succès.

4. Description textuelle de cas d'utilisation : **Signer document**

TABLE 3.4 – Description contextuelle de cas d'utilisation Signer document

Titre	Signer document
Résumé	Ce cas d'utilisation permet aux utilisateurs de signer leurs documents
Acteur	Autorité de certification, Administrateur, Système externe, Utilisateur
Pré-condition	l'application doit être lancer (page d'accueil) et l'utilisateur est authentifié
Scenario nominal	1) un utilisateur peut signer son document en cliquant simplément sur le bouton Signer document, 2) le système lui renvoi le formulaire à remplir 3) il téléverse son fichier(txt, docs, pdf,etc) 4) ensuite il téléverse sa clé publique 5) il sélectionne la fonction de hachage (ex. SHA1, SHA256 ...) 6) il valide en cliquant sur le bouton Signer document
Enchaînement Alternatif	l'algorithme est incorrect. l'enchaînement commence au point 2 du scénario nominal.
Enchaînement d'Erreur	E1 : Si l'étape 3 de scenario nominal est incorrect, un message d'erreur sera affiché. Si l'étape 4 de scenario nominal est incorrect, un message d'erreur sera affiché.
Post condition	La signature est effectuée avec succès.

5. Description textuelle de cas d'utilisation : **Envoyer Document**

TABLE 3.5 – Description contextuelle de cas d'utilisation Envoyer Document

Titre	Envoyer Document
Résumé	Ce cas d'utilisation permet aux utilisateurs d'envoyer leurs document signer
Acteur	Administrateur, Utilisateur
Pré-condition	l'application doit être lancer (page d'accueil) et l'utilisateur est authentifié
Scenario nominal	1) un utilisateur peut envoyer un document en cliquant sur l'onglet message **Envoyer document** 2) le système lui renvoi le formulaire à remplir 3) il téléverse son document 4) il téléverse son certificat 5) ensuite il choisit un destinateur 6) enfin il valide en cliquant sur le bouton **Envoyer**.
Enchaînement Alternatif	l'adresse E-mail est incorrect. l'enchaînement commence au point 2 du scénario nominal.
Enchaînement d'Erreur	E1 : Si l'étape 5 de scenario nominal est incorrect, un message d'erreur sera affiché.
Post condition	L'envoi est effectué avec succès.

6. Description textuelle de cas d'utilisation : **Chiffrer/Déchiffrer**

TABLE 3.6 – Description contextuelle de cas d'utilisation Chiffrer/Déchiffrer

Titre	Chiffrer/Déchiffrer
Résumé	Ce cas d'utilisation permet aux utilisateurs chiffrer/déchiffrer leurs documents
Acteur	Administrateur, Utilisateur et système externe
Pré-condition	l'application doit être lancer (page d'accueil) et l'utilisateur est authentifié
Scenario nominal	1) un utilisateur peut chiffrer/déchiffrer un document en cliquant sur le bouton **chiffrer/déchiffrer** 2) le système lui renvoi le formulaire à remplir 3) il téléverse son document 4) il téléverse sa clé publique 5) il choisit l'algorithme et la taille 6) enfin il valide en cliquant sur le bouton **chiffrer/déchiffrer**.
Enchaînement Alternatif	l'algorithme est incorrect. l'enchaînement commence au point 2 du scénario nominal.
Enchaînement d'Erreur	E1 : Si l'étape 5 de scenario nominal est incorrect, un message d'erreur sera affiché.
Post condition	Le chiffrement/déchiffrement est effectué avec succès.

Diagramme de classes

Diagramme de classe est considéré comme le plus important de la modélisation orienté objet, il est le seul obligatoire lors d'une telle modélisation. Il permet de fournir une représentation abstraite des objets du système qui vont interagir pour réaliser les cas d'utilisation. Le diagramme de classe modélise les concepts du domaine d'application ainsi que les concepts internes crées de toutes pièces dans le cadre de l'implémentation d'une application. Les principaux éléments de cette vue statique sont les classes et leurs relations : associations, généralisations et plusieurs types de dépendances, telles que la relation et l'utilisation.

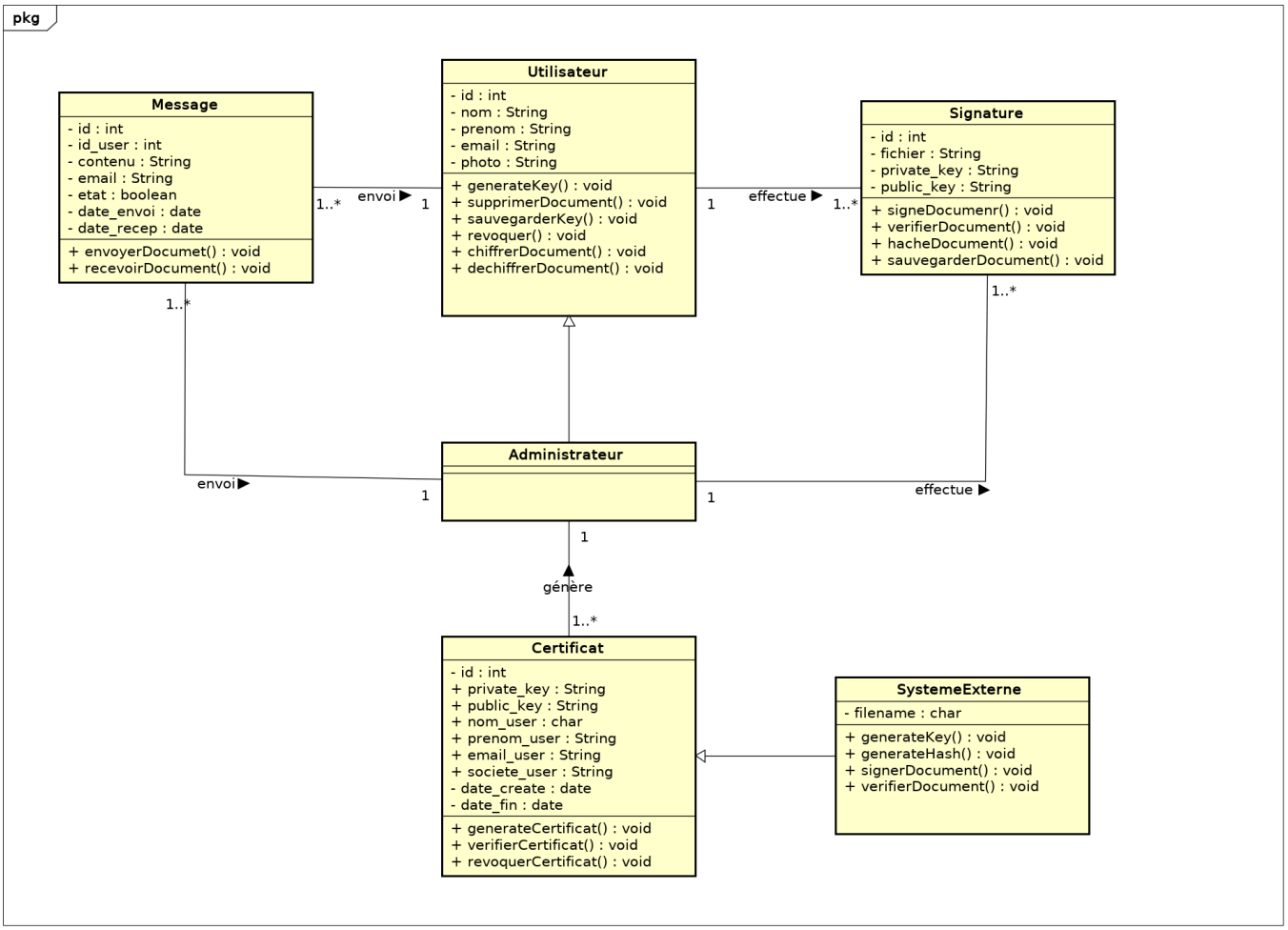

FIGURE 3.8 – Diagramme de classe

Diagramme de packages

Lorsque nous sommes en présence d'un système de grande taille, il peut être intéressant de le décomposer en plusieurs parties (appelées paquetage). Un paquetage est donc un regroupement de différents éléments d'un système (regroupement de classes, diagrammes, fonctions, interfaces...). Cela permet de clarifier le modèle en l'organisant. Il est représenté par un dossier avec son nom à l'intérieur.

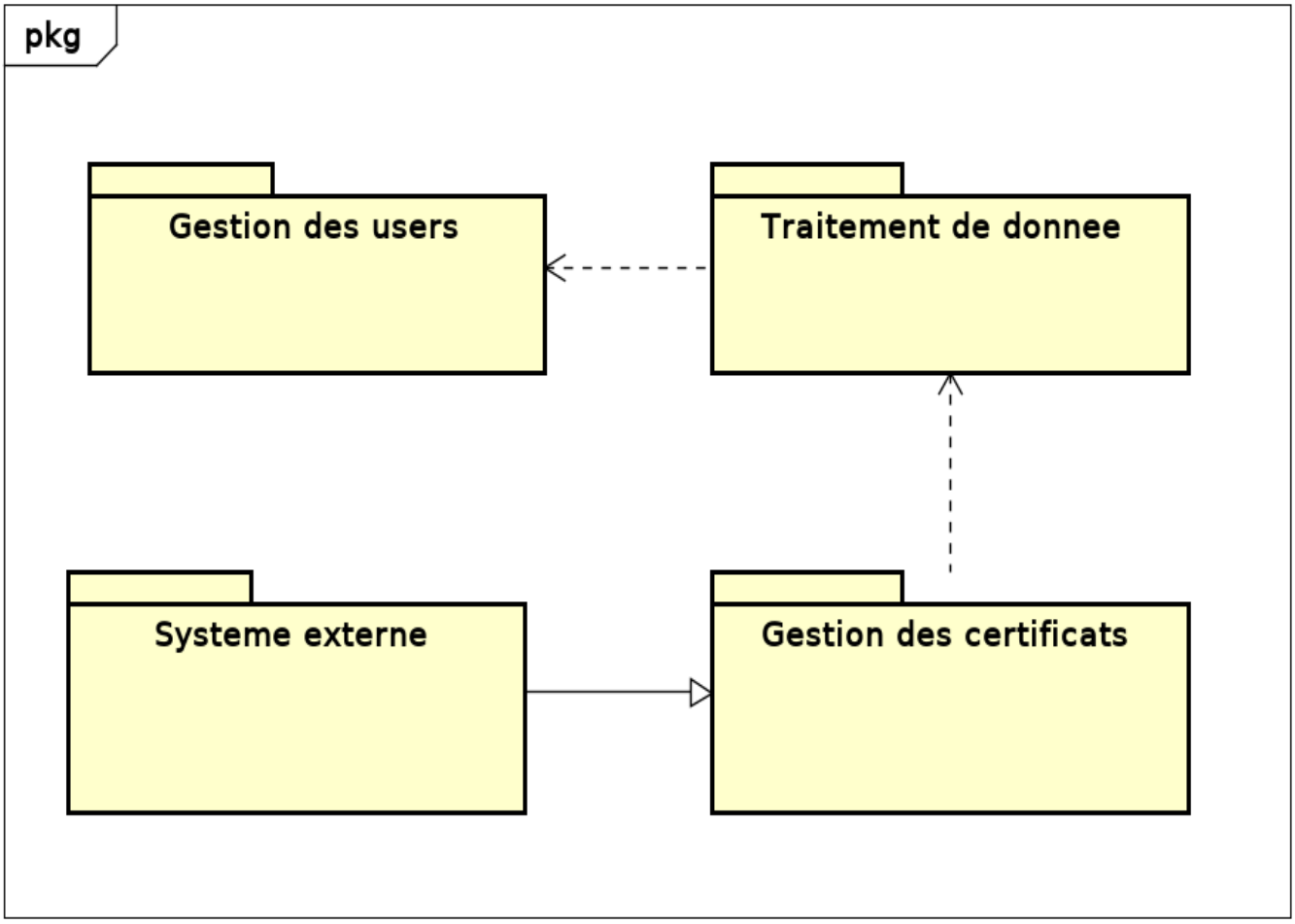

FIGURE 3.9 – Diagramme de packages

Diagramme de séquences

Pour décrire un scenario, UML propose un diagramme de séquences qui permet de décrire une séquence des messages échangés entre différents objets. Les diagrammes de séquences permettent de décrire comment les éléments du système interagissent entre eux et avec les acteurs. Les objets d'un système interagissent en s'échangeant des messages. Les acteurs interagissent avec le système au moyen d'interfaces homme-machine[**?**] .

1. **Diagramme de séquence de cas d'utilisation s'authentifier :**

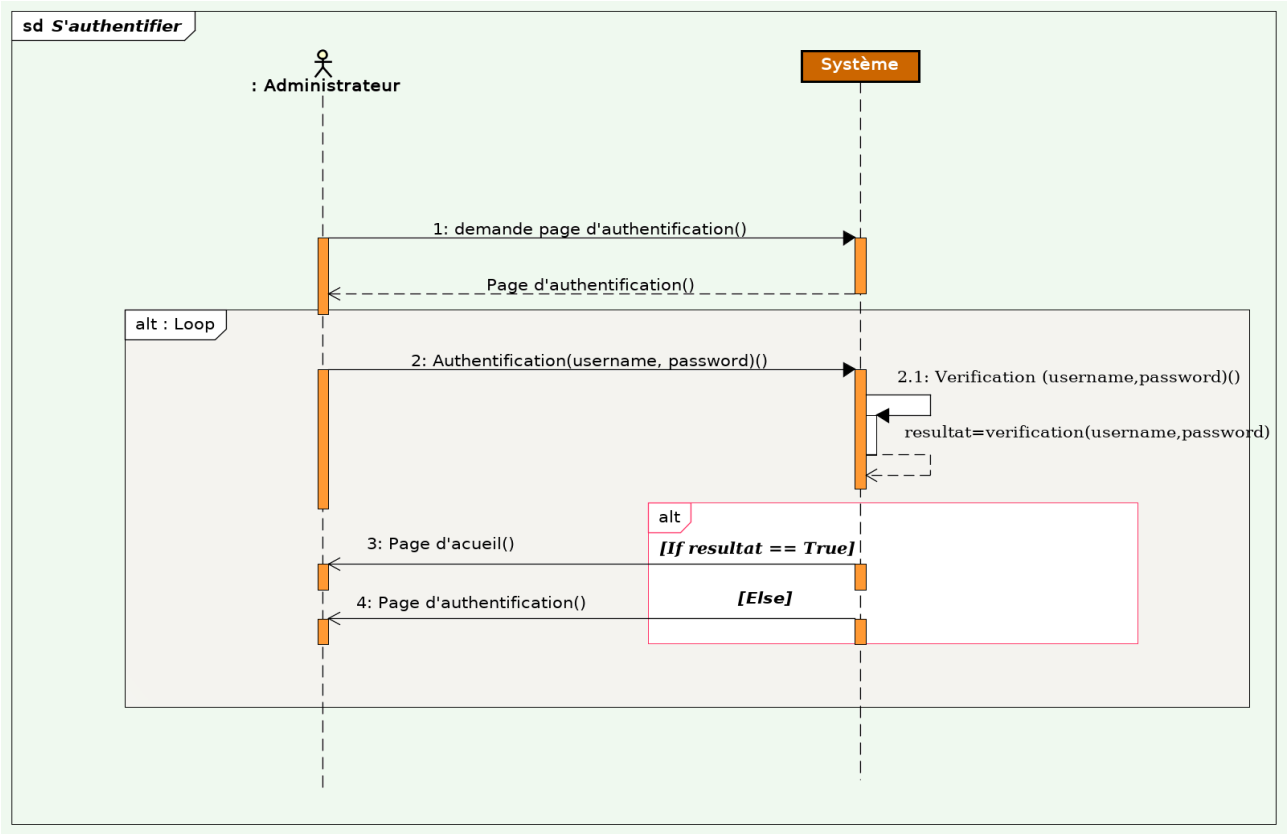

FIGURE 3.10 – Diagramme de séquence de cas d'utilisation s'authentifier

2. **Diagramme de séquence de cas d'utilisation générer key :**

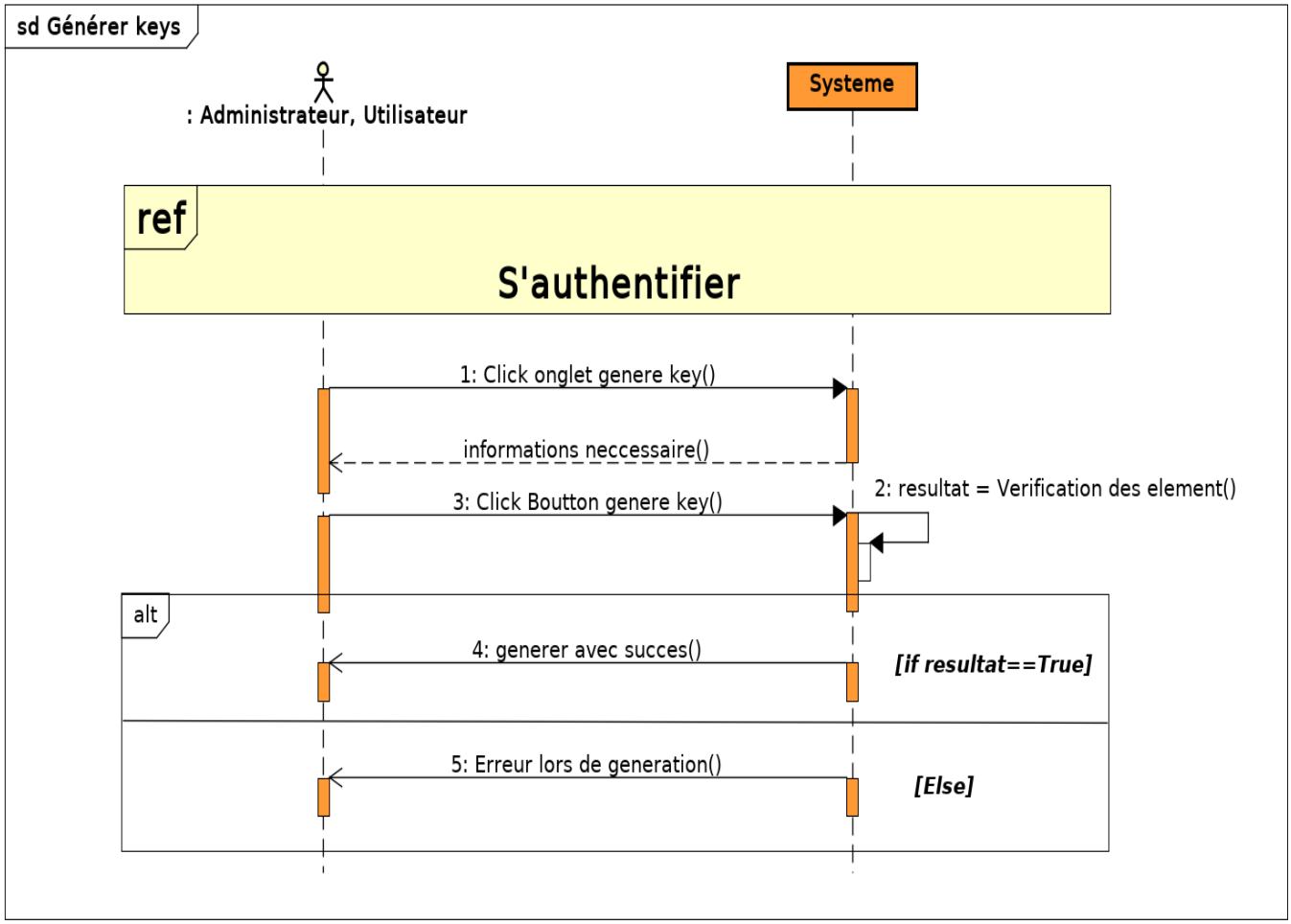

FIGURE 3.11 – Diagramme de séquence de cas d'utilisation générer key

3. Diagramme de séquence de cas d'utilisation certificat

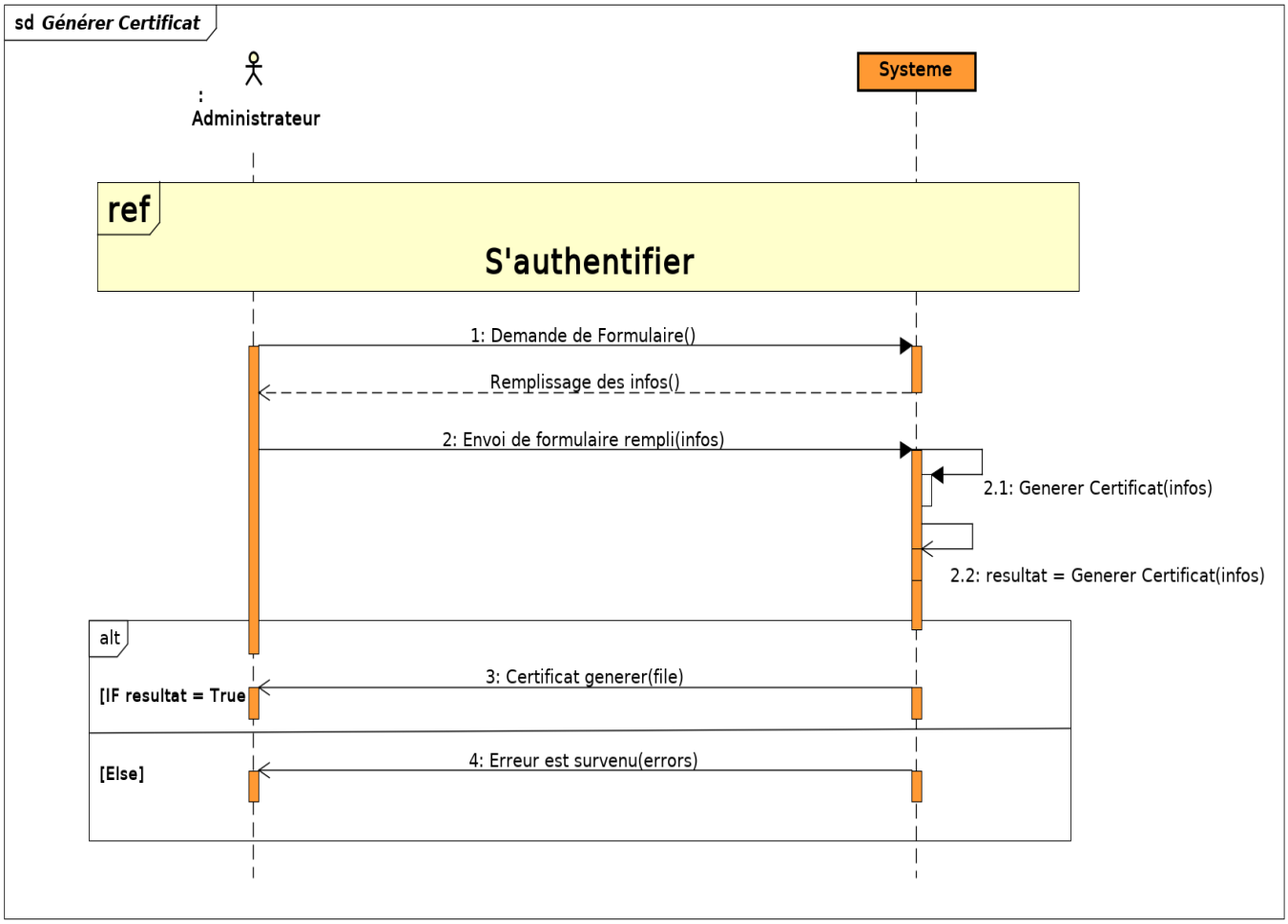

FIGURE 3.12 – Diagramme de séquence de cas d'utilisation générer certificat

4. **Diagramme de séquence de cas d'utilisation signer document :**

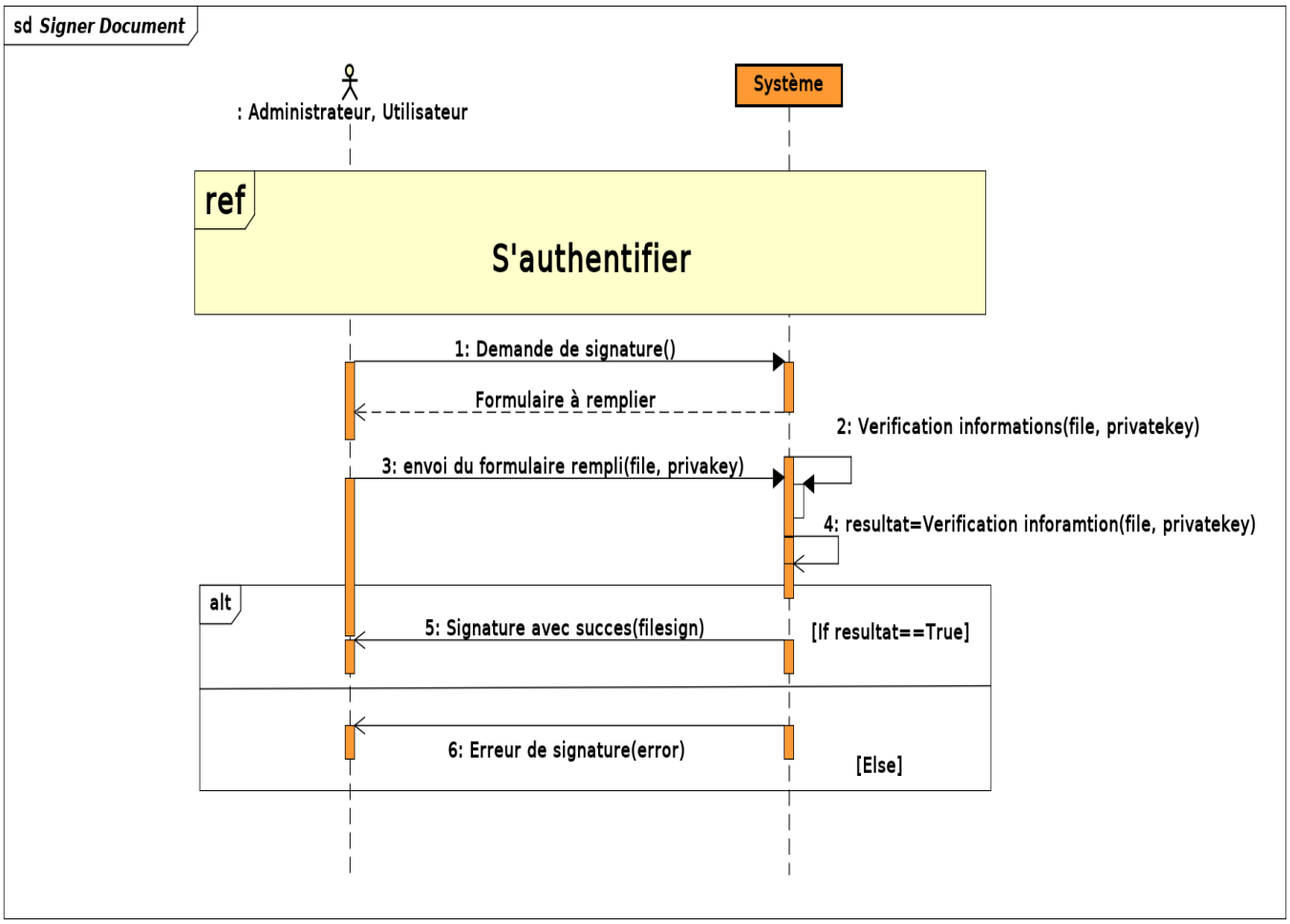

FIGURE 3.13 – Diagramme de séquence de cas d'utilisation signer document

5. **Diagramme de séquence de cas d'utilisation chiffrer/déchiffrer :**

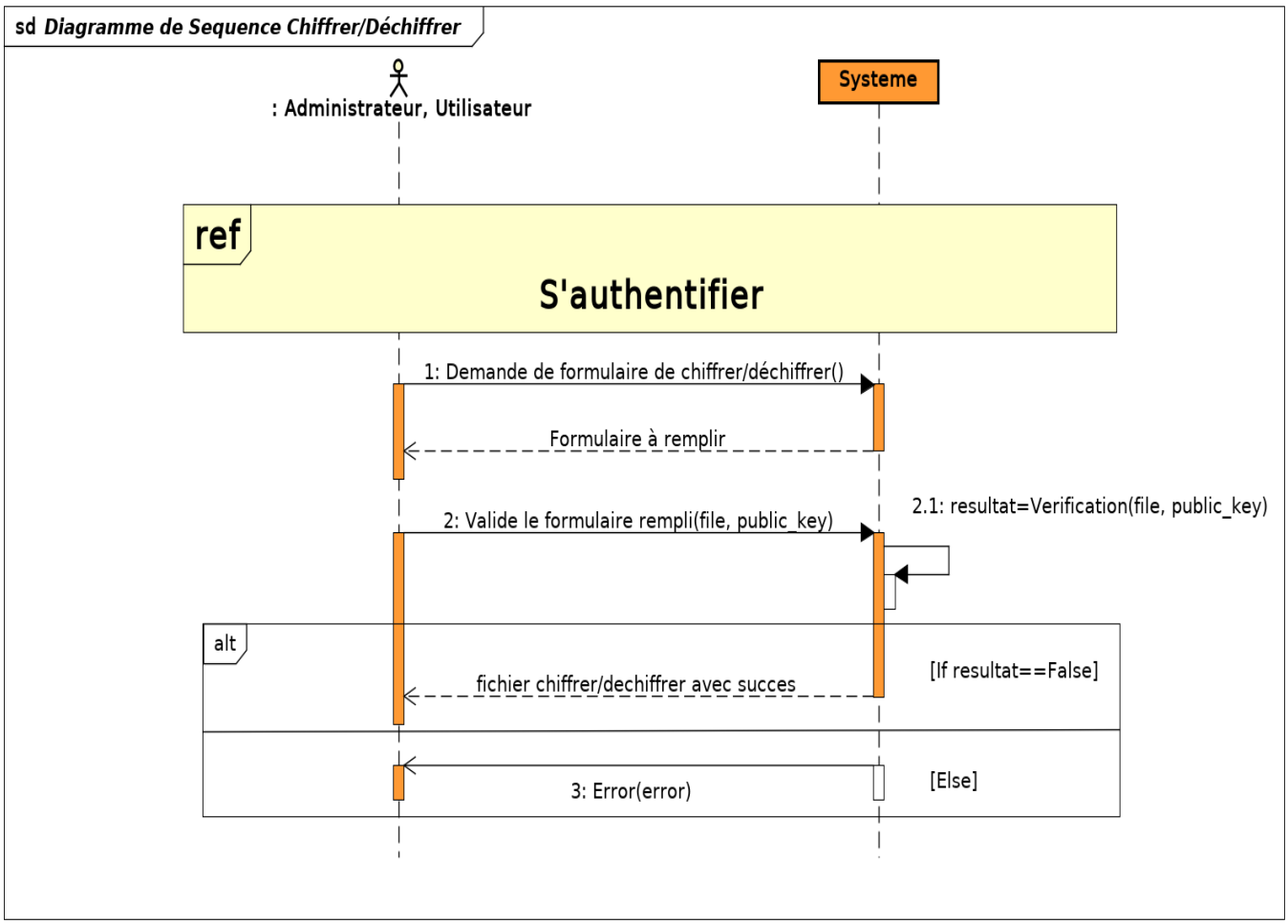

FIGURE 3.14 – Diagramme de séquence de cas d'utilisation signer document

6. **Diagramme de séquence de cas d'utilisation envoyer document :**

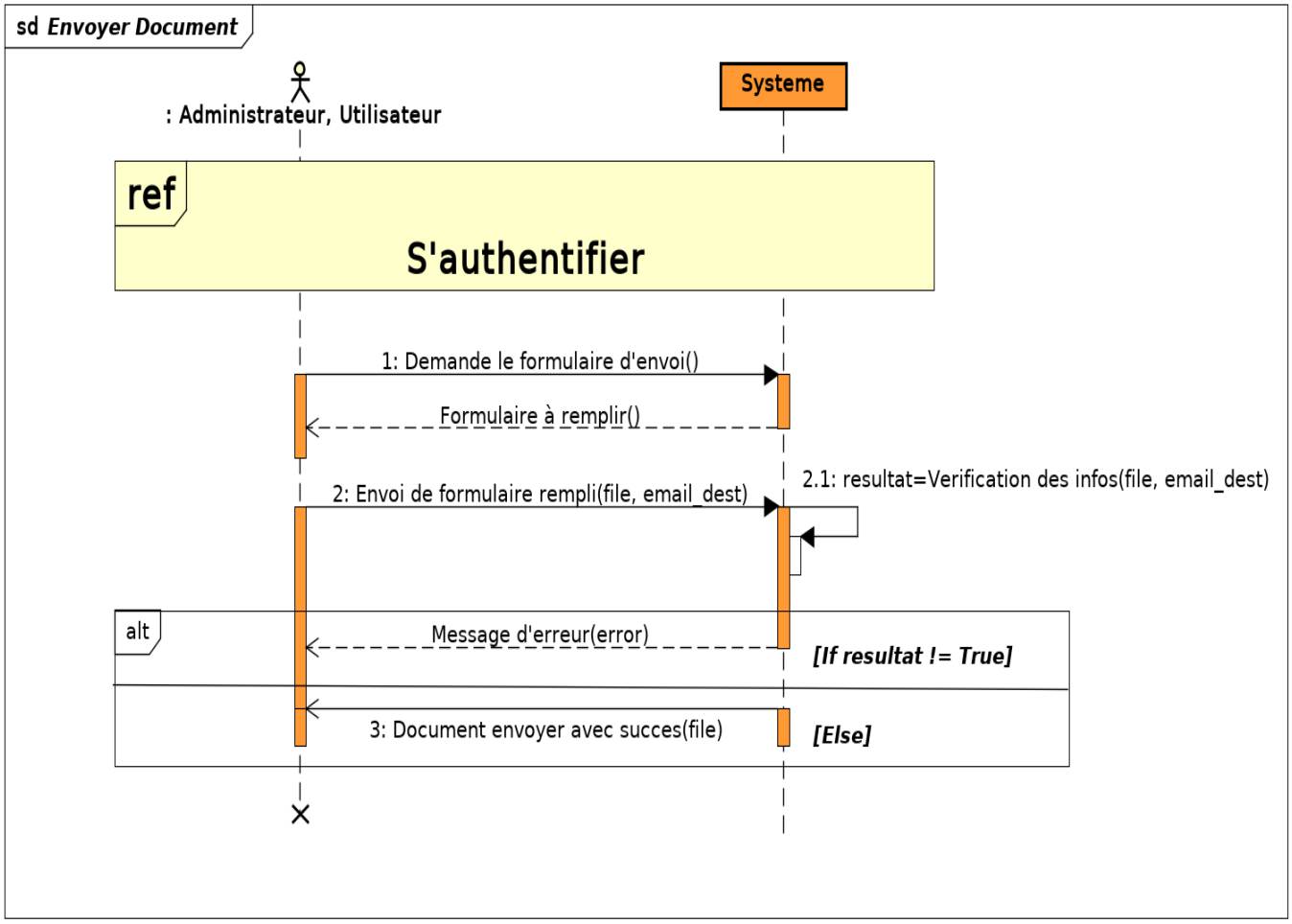

FIGURE 3.15 – Diagramme de séquence de cas d'utilisation envoyer document

Diagramme de déploiement

Dans le contexte du langage de modélisation unifié (UML), un diagramme de déploiement fait partie de la catégorie des diagrammes structurels, car il décrit un aspect du système même. Dans le cas présent, le diagramme de déploiement décrit le déploiement physique des informations générées par le logiciel sur des composants matériels. On appelle artefact l'information qui est générée par le logiciel[?].

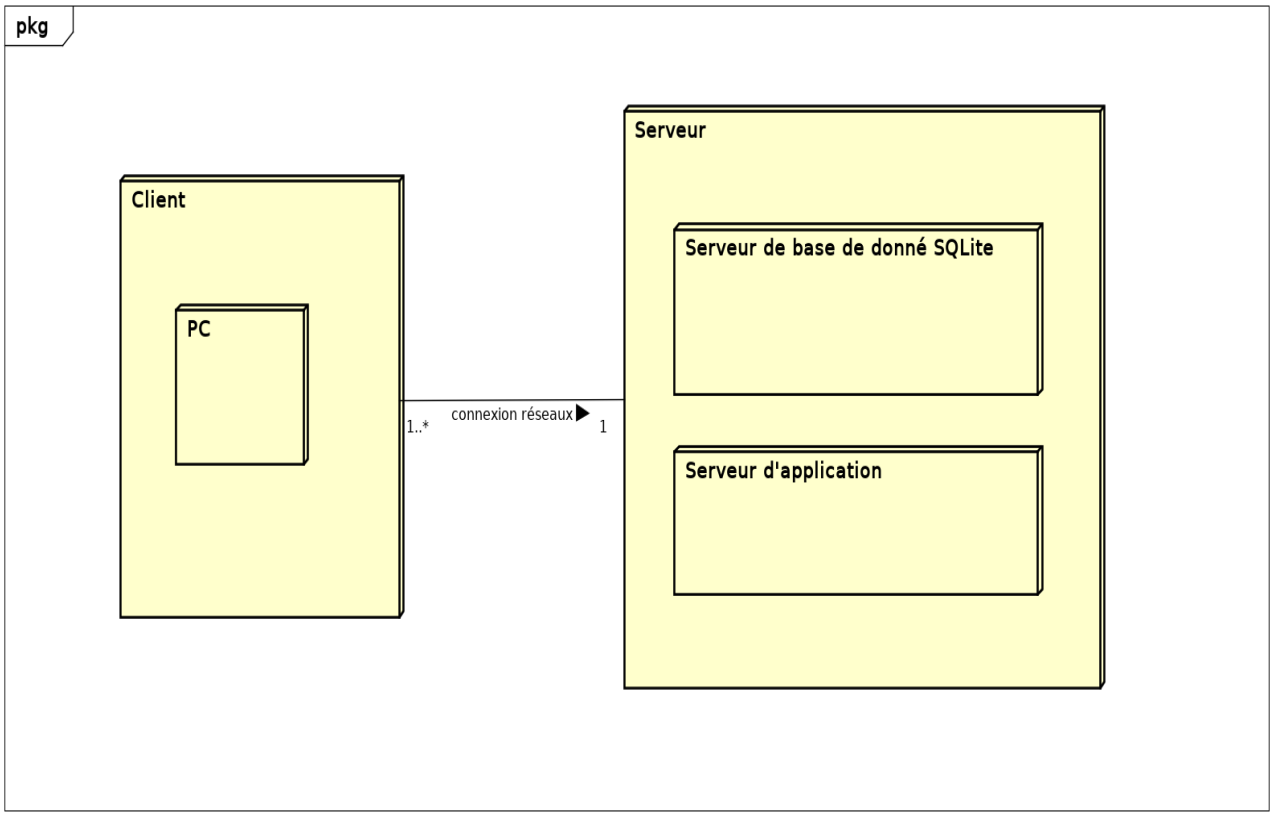

FIGURE 3.16 – Diagramme de séquence de cas d'utilisation envoyer document

Processus d'acquisition de certificat

Description...

3.7 Codage

3.7.1 Environnement de développement

3.7.2 Développement du module

3.7.3 Développement de l'interface utilisateur

Conclusion

Conclusion