

# 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 liée 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<sup>me</sup> 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 :

##### 1.1.4.1 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 maîtriser le risque qu'engendre le système d'information dans

le fonctionnement de toute organisation. Ainsi l'audit des systèmes d'information comme activité visant à mesurer le niveau de conformité d'un système d'information par rapport à des règles bien définies et à examiner le niveau de dérive du système par rapport à ces standards aide à anticiper sur les problèmes et à 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 fixés au départ. Le système d'information ne saurait faire exception à cette règle, au contraire nécessite plus d'attention dans ce sens car complexe et indispensable pour toute entreprise. Les investissements faits 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 liés à l'investissement en question.

#### 1.1.4.2 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<sup>1</sup> 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 mécanismes de protection de données 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

#### 1.1.4.3 Formations

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

- sécurité des systèmes d'information ;

---

<sup>1</sup>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 agréé 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 formations dans les salles.

Le centre donne l'accès gratuit et illimité aux forums et discussions via le portail web linkedin ([www.linkedin.com](http://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.

#### 1.1.4.4 Certifications

ITS offre également des certifications suivantes :

##### 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)

#### 1.1.4.5 Produits

L'entreprise a mis à la disposition de tout le monde des logiciels gratuits, on peut citer entre autres 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**.

#### 1.1.5.1 Situation géographique

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

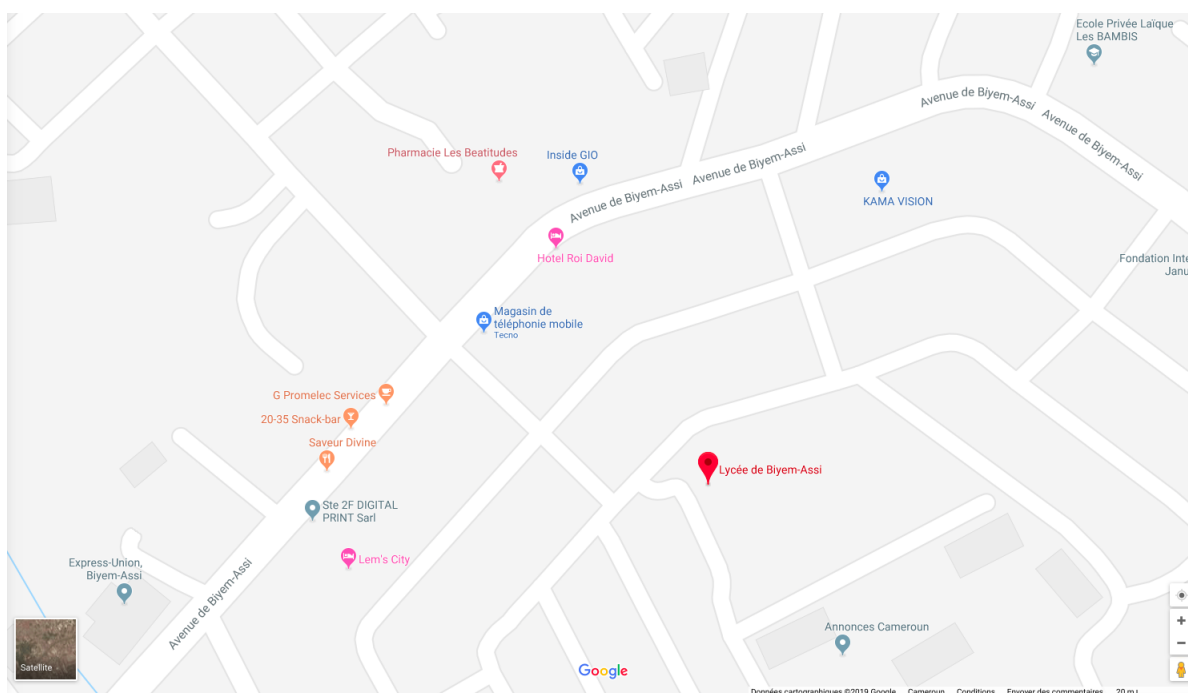


FIGURE 1.1 – Situation géographique du lieu de stage

## 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.