

*Préambule : cet article est rédigé dans le cadre du stage obligatoire de deuxième année de Bachelor Informatique chez Lyon Ynov Campus. Ce stage a pour objectif de mettre en pratique les connaissances acquises durant la formation et de découvrir le monde professionnel.*

*Dans la mesure où la date de fin de stage est fixée au-delà de la deadline pour le rendu du rapport, celui-ci sera nécessairement incomplet lors du rendu de celui-ci. Les expériences consignées seront celles réalisées avant la date de rendu du rapport.*

## Partie 1 : le cadre du stage

---

### 1.1 Contexte

---

Le stage se déroule au sein du Campus RTE Jonage, qui est le centre de formation du gestionnaire de transport d'électricité RTE. Le stage se déroule sur la période allant du 11 août 2025 au 23 septembre 2025 inclus. Son encadrement est assuré par M. Jean-Luc Toupet, chargé d'affaires immobilier et logistique.

### 1.2 Objectifs du stage

---

Tels qu'établis par la Convention de stage signée par les deux parties (Lyon Ynov Campus et RTE), le programme du stage est le suivant :

"Le stage correspond à une période temporaire de mise en situation en milieu professionnel au cours de laquelle le Stagiaire acquiert des compétences professionnelles et met en œuvre les acquis de sa formation en vue de l'obtention d'un diplôme ou d'une certification et de favoriser son insertion professionnelle. Le Stagiaire se voit confier une ou des missions conformes au projet pédagogique défini par son établissement d'enseignement et approuvées par l'entreprise d'accueil.

L'entreprise d'accueil doit confier au Stagiaire, en accord avec l'établissement d'enseignement ou l'organisme de formation, des tâches et des responsabilités en rapport direct avec les qualifications et les compétences auxquelles conduit le diplôme préparé ou la formation suivie.

Le contenu du cadre ci-dessous doit être défini conjointement par les responsables du Stagiaire dans l'établissement d'enseignement ou l'organisme de formation et par l'entité encadrant le stagiaire de l'entreprise d'accueil.

Objectifs pédagogiques du stage et compétences pédagogiques :

Ce stage a pour objectif principal de permettre au stagiaire de mettre en œuvre ses connaissances en informatique et en cybersécurité dans un contexte professionnel

concret.

Il vise à :

- Comprendre les enjeux de la sécurité physique et logique dans un environnement complexe.
- Appliquer des méthodes d'analyse des besoins métiers en matière de sécurité d'accès.
- Concevoir une solution sécurisée et adaptée aux différents profils d'utilisateurs.
- Modéliser une base de données en lien avec les accès physiques.
- Produire un livrable structuré et exploitable par les équipes techniques.

Pour atteindre cet objectif, le stagiaire devra :

- Analyser des besoins et rédiger un cahier des charges.
- Cartographier des accès et modéliser des systèmes complexes.
- Concevoir et sécuriser une base de données.
- Communiquer et rédiger des livrables techniques.
- Collaborer avec des équipes pluridisciplinaires.

Sujet précis du stage : Refonte du système de badges d'accès pour sécuriser un site multi-bâtiments et répondre aux besoins spécifiques des différents métiers.

En effet le site concerné est composé de 9 bâtiments aux usages variés : plateformes techniques, bureaux, espaces de formation, halles techniques, ateliers, locaux avec habilitation électrique, sous-sols techniques, etc. Les utilisateurs sont internes (DSIT, formation, expertise réseau, R&D) et externes (visiteurs, stagiaires, formateurs, direction, logistique), chacun avec des besoins d'accès spécifiques.

Partie théorique du stage : La partie théorique du stage consistera à :

- Étudier les principes de sécurité physique et logique des accès.
- Analyser les normes et bonnes pratiques en cybersécurité des infrastructures.
- Comprendre les enjeux de segmentation des accès selon les profils métiers.
- Se former à la modélisation de bases de données relationnelles adaptées à la gestion des accès.
- Étudier les solutions existantes de contrôle d'accès et leur intégration dans un SI.

Partie appliquée du stage : La partie appliquée comprendra les étapes suivantes :

1. Recueil des besoins métiers : entretiens avec les représentants des différents métiers pour identifier les besoins d'accès spécifiques.
2. Cartographie des accès : représentation graphique des bâtiments, des espaces et des flux d'accès.
3. Modélisation de la base de données : conception d'un schéma relationnel permettant de gérer les profils, les droits d'accès et les zones sécurisées.

4. Rédaction du livrable : document détaillant les profils types, les accès associés, les cas particuliers et les recommandations de sécurité.
5. Initialisation de la base de données : si nécessaire, intégration des données dans le SI existant et tests de cohérence.

Compétences mobilisées :

- Cybersécurité : principes de sécurité des accès, gestion des identités, segmentation des droits.
  - Base de données : conception, modélisation, initialisation, requêtage.
  - Analyse métier : compréhension des besoins, formalisation, priorisation.
  - Communication : rédaction de livrables, présentation des résultats, collaboration interservices, recueil des besoins.
  - Gestion de projet : planification, suivi des étapes, validation des livrables."
- Source : ARTICLE 3 "PROGRAMME DU STAGE" du document CONVENTION DE STAGE fourni par RTE et signé par l'école, pages 2-3/10

Un beau programme, en somme.

## 1.3 Échanges préparatoires avec RTE et hypothèses subséquentes

---

Plusieurs échanges, dont un en visioconférence, ont eu lieu préalablement au commencement du stage afin de clarifier les attentes et les objectifs du projet. La problématique était la suivante : comment refondre le système des profils du système de contrôle d'accès pour quelque chose de moins monolithique ? Selon le service de gestion immobilière et logistique, les problèmes remontés par le PC sécurité étaient qu'il existait trop de profils d'accès différents. Je devais donc simplifier le système en question vers quelque chose de plus modulaire.

*Je précise que le passage qui suit concerne mes hypothèses de départ. Bien que certaines d'entre elles furent pour la plupart confirmées, je consigne celles-ci afin de prêter directement au lecteur du présent rapport la perspective à partir de laquelle j'abordais ce stage.*

Tel que je comprenais le problème, il semblait que je devais recoder une interface de gestion des contrôles d'accès qui communiquerait avec un serveur central dont j'ignorais la nature, auquel auraient accès les agents du PC sécurité, qui inclurait des gestions de groupes, le tout dans un environnement multi-bâtiments. L'idée que je m'en faisais, c'était celle d'un réseau de badgeuses organisées autour d'un serveur hébergé côté SI, avec lequel interagiraient les agents du PC-sécu à travers une interface web simple d'utilisation. Les requêtes allaient très probablement être au format HTTP vers une API REST, que j'aurai à reverse-engineer (alerte néologisme foireux), décortiquer, et reproduire sur un client web fait maison, capable d'envoyer les requêtes HTTP contenant les rôles des différentes personnes ayant accès au site et à ses parties. J'aurai probablement à travailler sur une refonte complète des rôles et des

différents accès, basés sur comme nous le verrons plus tard, les besoins d'un campus de 15000m<sup>2</sup>, 300 employés et 7000 élèves (une bagatelle, quoi), impliquant potentiellement la mise en place d'une base de données qui me permettrait de mettre en relation les informations des utilisateurs avec celles des badgeuses, des rôles, des badges et des espaces.

C'est ce que je pouvais déduire en croisant les impératifs de ma convention de stage avec les informations recueillies lors des échanges préparatoires. Du sacré boulot.

## 1.4 Premier jour

---

Arrivée sur site à 8h-20. Je fais la connaissance de M. Toupet, mon tuteur de stage. Je connais déjà le campus de par un stage précédent, il m'emmène donc directement au PC sécurité où se trouve les futurs exploitants de mon livrable. Ceux-ci m'expliquent la partie de leur travail qui concerne le mien avec démonstrations à l'appui. Leur logiciel, **AEOS**, est très complet. On peut y attribuer plusieurs "profils" à un utilisateur (un profil étant une collection de droits d'accès regroupés dans un ensemble cohérent). Je me vois donc délesté du travail que je me voyais réaliser pendant le stage. Le véritable problème, très vite pointé du doigt par les agents du PC-sécu, est la surabondance de profils dans la base de données d'où ils peuvent les attribuer, et l'impossibilité d'éditer, créer ou supprimer ceux-ci sans certains droits qu'ils ne possédaient pas. Les droits en question étaient gérés par leurs collègues du service Multi-Technique, géré par des prestataires employés par VINCI (une branche spécialisée dans les services de la célèbre société de gestion des autoroutes). Il m'était également imparti, en outre, de répertorier sous des appellations cohérentes tous les systèmes de contrôle d'accès installés à titre provisoire puis conservés à titre permanent.

## 1.5 Objectifs de mission

---

Les besoins de la mission sont donc les suivants :

1. Enumérer l'ensemble des profils de droits d'accès et identifier pour chacun d'entre eux les entités dont elles découlent
2. Répertorier les systèmes de contrôle d'accès installés à titre provisoire puis conservés à titre permanent
3. Penser une refonte plus modulaire du système de profils afin que ceux-ci ne se superposent pas.
4. Consulter les responsables des différentes entités sur le campus à propos de leurs besoins, proposer un plan de refonte des profils en supprimant les profils redondants et en en créant de nouveaux si nécessaire.
5. Documenter l'ensemble du processus et des décisions prises afin de faciliter la maintenance et l'évolution future du système.
6. Demander l'approbation de mon tuteur (et gestionnaire de stage) vis-à-vis du plan de refonte des accès.

7. Préparer une backup de la base de données des profils d'accès avant toute modification.
8. Envoyer au responsable du service Multi-Technique un rapport détaillé sur les profils d'accès et les systèmes de contrôle d'accès en place à modifier et mettre en place, ainsi que les recommandations pour leur refonte.